ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМАХ С ЦИФРОВЫМИ ЭЛЕКТРОННЫМИ УСТРОЙСТВАМИ, СИСТЕМАМИ ЗАЩИТЫ, АВТОМАТИКИ И УПРАВЛЕНИЯ

Гурина Л.А., к.т.н., доцент, с.н.с. Лаборатории управления функционированием электроэнергетических систем ИСЭМ СО РАН, Иркутск

Куликов А.Л., д.т.н., профессор кафедры «Электроэнергетика, электроснабжение и силовая электроника» НГТУ им. Р.Е. Алексеева, Нижний Новгород

2025

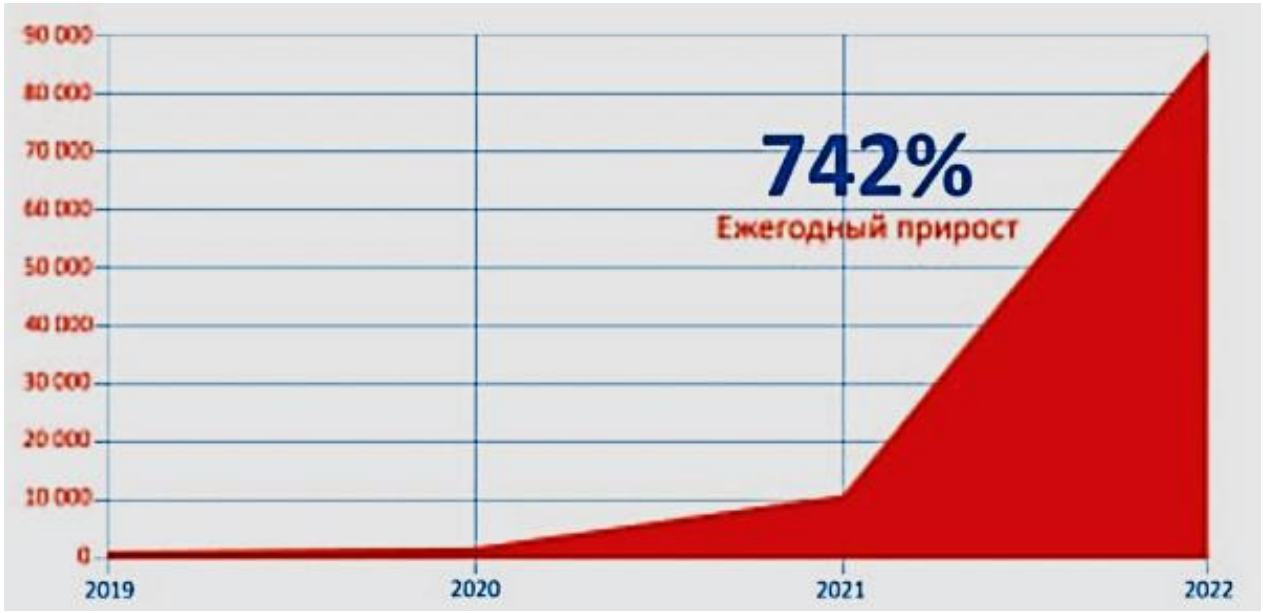
1. Анализ нормативной базы в области информационной безопасности и доверенные программно-аппаратные комплексы.
2. Оценка рисков кибербезопасности при управлении ЭЭС.
3. Методы повышения качества информации при управлении ЭЭС в условиях кибератак.
4. Методика оценки устойчивости информационных систем ЭЭС при кибератаках.
5. Обеспечение кибербезопасности при вторичном регулировании напряжения в системах управления микросетями.

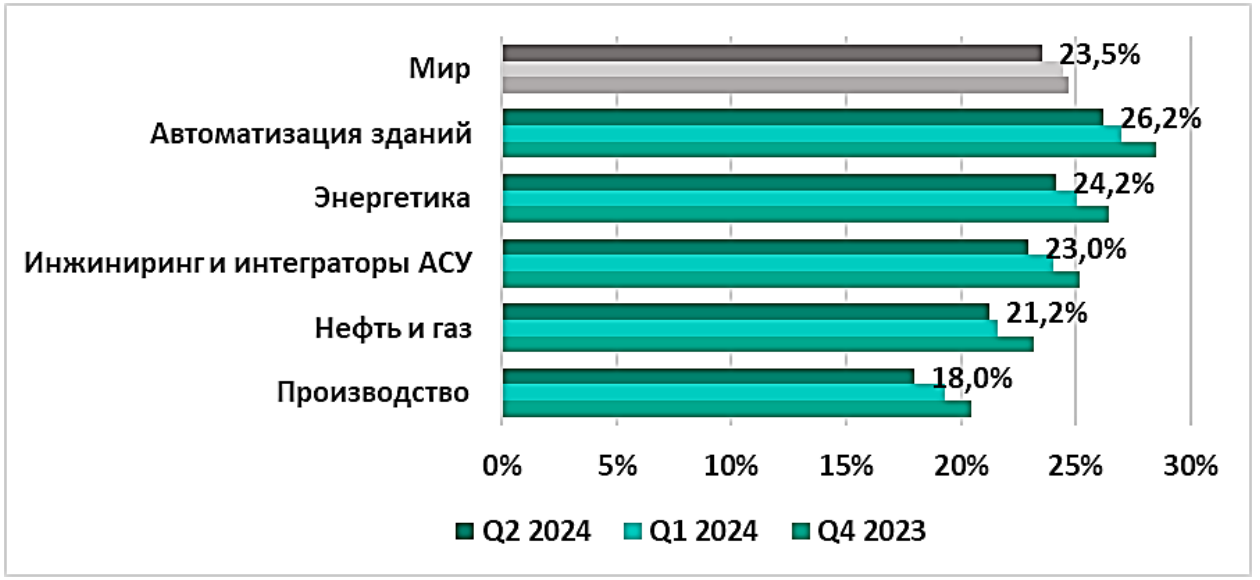
В электроэнергетике России наблюдаются два процесса трансформации: переход к распределенной энергетике и цифровизация. ЭЭС претерпевают радикальные изменения своих свойств как за счет трансформации своей внутренней структуры, так и за счет использования инновационных технологий производства, передачи, хранения, распределения и потребления электроэнергии. **Цифровая трансформация объектов энергетики, использование интеллектуальных методов управления обусловливает появление ЭЭС с большим многообразием цифровых объектов, начиная от внедрения цифровых устройств до появления цифровых систем управления, релейной защиты и автоматики и способствует успешной реализации кибератак (КА).**

Становятся актуальными **вопросы обеспечения устойчивости цифровых объектов ЭЭС при кибератаках** упреждающим комплексным реагированием на эти угрозы.

Для сохранения надежного функционирования ЭЭС в условиях современных вызовов и угроз необходима разработка методов управления, создающих возможности робастности, адаптации и восстановления объектов при возникновении отказов и сбоев в результате кибератак.

Статистика кибератак в России





Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты, в некоторых отраслях

https://ics-cert.kaspersky.ru/publications/reports/2024/09/26/threat-landscape-for-industrial-automation-systems-q2-2024/

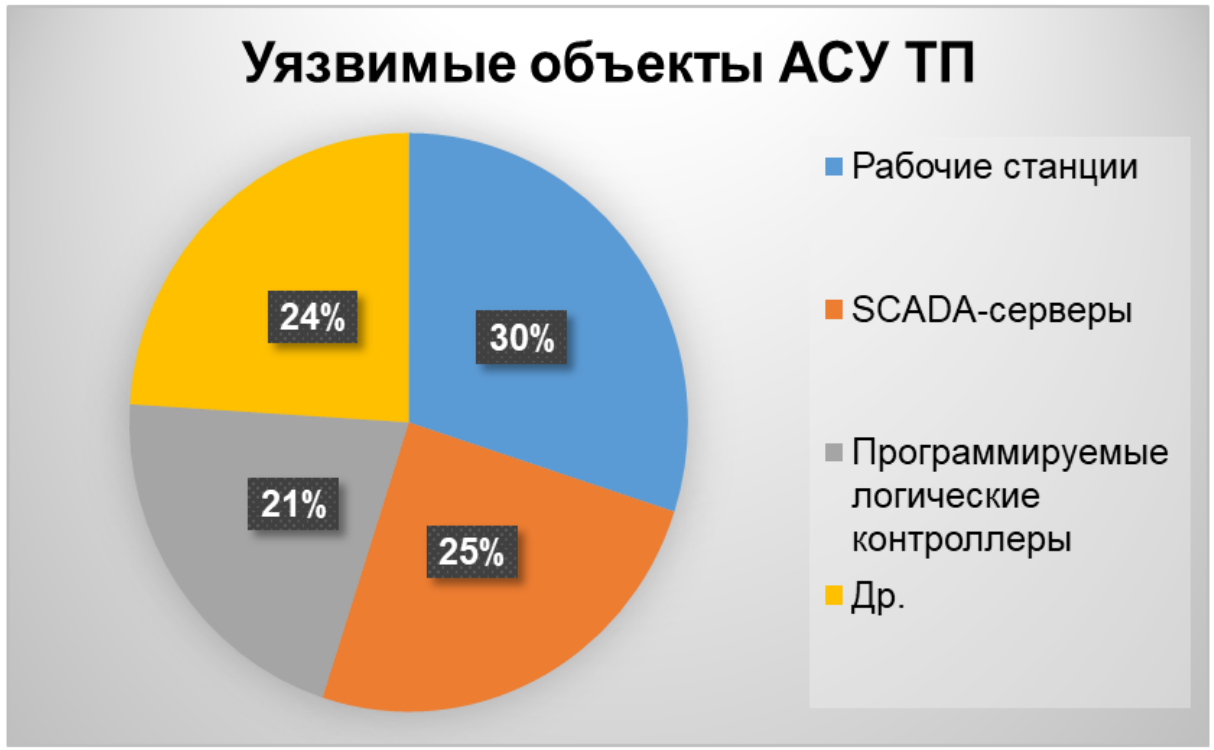
«Наибольший интерес у киберпреступников вызывают распределенные структуры — энергетические и транспортные компании, а также предприятия с удаленными объектами…»

Источник: https://www.anti-malware.ru/news/2025-02-27-121598/45390

Хакеры атаковали энергокомпанию в Ленобласти и пытались отключить свет

Санкт-Петербург, 17 октября, 2022, 12:34 — ИА Регнум. Злоумышленники совершили массированную кибератаку с попыткой взломать сетевую структуру АО «ЛОЭСК» и отключить свет в Ленинградской области, но их атаку удалось отразить, сообщили 17 октября в пресс-службе компании.

За 2023 – 2024 гг. число атак на АСУ ТП в России выросло на 160%.



В 70% случаев атаки сопровождаются внедрением троянцев-вымогателей

Источник: https://www.anti-malware.ru/news/2025-02-27-121598/45390

Major cyberattacks on the energy industry 2023

January

CDN Jan 15
Baker Lake / ᖃᑲL..., NU
Energy supply compa...

February

I Feb 02
Roma
Energy supply compa...

BR February
Rio de Janeiro
Service provider

D February
Karlsruhe
Utility

USA February
Houston, TX
Oil and gas produce...

March

CH March
Zurich, ZH
Technology company

April

CDN Apr 13
Montreal, QC
Energy supply compa...

PE Apr 17
Arequipa
Energy supply compa...

May

DK May
Energy companies

IND May 22
Jabalpur / जबलपुर
Energy supply compa...

D May 31
Munich
Energy technology

NL May 31
The Hague
Petroleum company

NL May 31
Arnhem
Power grid operator

OM May 31
Oman
Oil and gas

UK May 31
United Kingdom
Oil and gas

USA May 31
Oak Ridge, TN
Consortium of unive...

USA May 31
USA
Energy supply

USA May 31
Houston, TX
Logistics

USA May 31
USA
Oil and gas

USA May 31
Houston, TX
Oil and gas

USA May 31
Carlsbad, NM
Radioactive waste r...

USA May 31
Austin, TX
Service provider

June

D June
Güglingen
Solar parks

CDN Jun 23
Calgary, AB
Petroleum company

July

IL July
Haifa / חֵיפָה
Oil refinery

August

AUS Aug 18
Sydney, NSW
Service provider

F August?
Paris
Energy supply compa...

October

D October?
Meschede
Energy supply compa...

November

USA Nov?
Idaho Falls, ID
Nuclear research la...

SLO Nov 22
Ljubljana
Energy supply compa...

D Nov
Gevelsberg
Energy supply compa...

CDN Nov
Richmond Hill, ON
Pipeline operator

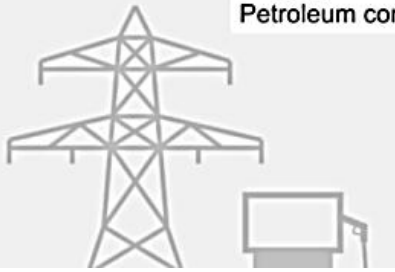
December

CU Dec?
Willemstad
Utility

DK Dec 09
Holstebro
Energy supply compa...

IR Dec 18
Iran
Petrol stations

USA Dec?
Afton, WY
Energy supply compa...



ENISA: в 2023 году зарегистрировано **более 200 киберинцидентов, направленных на энергетический сектор,** и более половины из них были направлены на Европу.

Целью исследования является разработка методов обеспечения кибербезопасности информационных систем при управлении режимами электроэнергетических систем с цифровыми электроэнергетическими объектами, системами управления, релейной защиты и автоматики в условиях новых вызовов и угроз.

Объектом исследования являются цифровые электроэнергетические объекты.

Предметом исследования являются методы обеспечения кибербезопасности на цифровых электроэнергетических объектах, входящих в состав ЭЭС.

1. АНАЛИЗ НОРМАТИВНОЙ БАЗЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ДОВЕРЕННЫЕ ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ

Актуальность проблемы обеспечения ИБ обусловлена следующими факторами:

- **быстрые темпы роста количества различных электронных устройств**, применяемых в самых разных сферах деятельности, и, как следствие, резкое расширение круга пользователей, имеющих непосредственный доступ к сетям и информационным ресурсам;
- **резкое увеличение объемов информации**, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
- **бурное развитие аппаратно-программных средств и технологий, не соответствующих современным требованиям безопасности**;
- **несоответствие развития средств обработки информации и проработки теории информационной безопасности**, разработки международных стандартов и правовых норм, **обеспечивающих необходимый уровень защиты информации**;
- **повсеместное распространение сетевых технологий, создание единого информационно-коммуникационного мирового пространства на базе Интернет** (например, «Интернет вещей (IoT)»), которая по своей идеологии не обеспечивает достаточного уровня информационной безопасности.
- **высокий ежегодный рост количества компьютерных преступлений** в мире и России и ущерба, причиняемого такими преступлениями.

С точки зрения правовых отношений **структурную модель информационной безопасности компьютерных систем** можно представить в виде схемы, показанной на рис.

Основными структурными элементами информационной безопасности компьютерных систем в данной модели являются:

1.Цели защиты информации
2.Субъекты, участвующие в процессах информационного обмена
3.Угрозы безопасности информационных систем
4.Уровни уязвимости информации и информационной инфраструктуры.

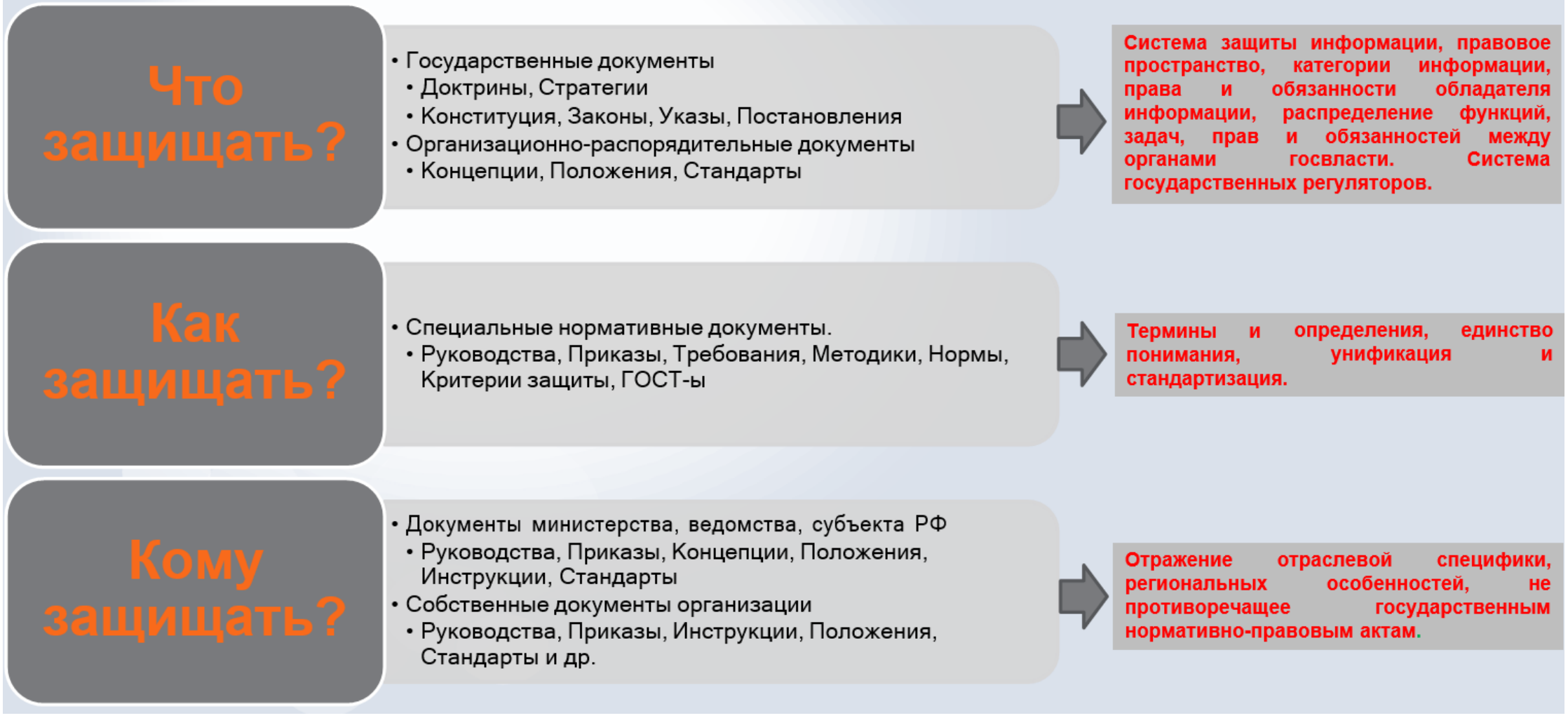
Обеспечение ИБ состоит в достижении 3-х взаимосвязанных целей – **целостность, доступность и конфиденциальность**.

Обеспечение конфиденциальности состоит в защите информации в процессе ее создания, хранения, обработки и обмена по каналам связи от ознакомления с ней лицами, не имеющими права доступа.

Обеспечение целостности состоит в защите от преднамеренного или непреднамеренного изменения информации и алгоритмов ее обработки лицами, не имеющими на то права.

Обеспечение доступности состоит в предоставлении авторизованным пользователям всей имеющейся в системе информации в соответствии с установленными правами доступа.

В настоящее время **для обеспечения защиты информации требуется не просто разработка частных механизмов защиты, а реализация системного подхода**, включающего в себя комплекс взаимосвязанных мер с использованием специальных аппаратно-программных средств, организационных мероприятий, нормативно-правовых актов.



Название	Дата принятия
О техническом регулировании	Федеральный закон от 27 декабря 2002 года № 184-ФЗ
Об информации, информационных технологиях и о защите информации	Федеральный закон от 27 июля 2006 года № 149-ФЗ
О государственной тайне	Закон РФ от 21 июля 1993 г. N 5485-I
О лицензировании отдельных видов деятельности	Закон РФ от 04.05.2011 № 99−ФЗ
Кодекс Российской Федерации об административных правонарушениях	От 30 декабря 2001 года № 195-ФЗ
Уголовный кодекс Российской Федерации	От 13 июня 1996 года № 63-ФЗ
Об электронной подписи	Федеральный закон от 6 апреля 2011 года № 63-ФЗ
О федеральной службе безопасности	Закон Российской Федерации № 40 от 3 апреля 1995г.
О персональных данных	Федеральный закон от 27 июля 2006 года № 152-ФЗ
О коммерческой тайне	Федеральный закон от 29 июля 2004 года N 98-ФЗ
О безопасности критической информационной инфраструктуры РФ	Федеральный закон от 26 июля 2017 года № 187-ФЗ

01.01.2018 вступил в действие **Федеральный закон № 187-ФЗ** «**О безопасности критической информационной инфраструктуры Российской Федерации**».

Согласно 187-ФЗ к **субъектам КИИ** относятся «**государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели**, которым на праве собственности, аренды или на ином законном основании принадлежат **информационные системы**, **информационно-телекоммуникационные сети**, **автоматизированные системы управления (объекты)**, **функционирующие в сфере** здравоохранения, науки, транспорта, связи, **энергетики**, банковской сфере и иных сферах финансового рынка, **топливно-энергетического комплекса**, **в области атомной энергии**, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей».

Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении **Правил категорирования объектов критической информационной инфраструктуры** Российской Федерации, а также **перечня показателей критериев значимости объектов критической информационной инфраструктуры** Российской Федерации и их значений»

Автоматизированная система управления - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

Безопасность КИИ - состояние защищенности КИИ, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

Значимый объект КИИ - объект КИИ, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов КИИ;

Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

Компьютерный инцидент - факт нарушения и (или) прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

КИИ - объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

Объекты КИИ - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ;

Субъекты КИИ - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, …, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

В соответствии с Указом Президента РФ от 16 августа 2004 г. N 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» **Федеральная служба по техническому и экспортному контролю (ФСТЭК России)** является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1. **обеспечения безопасности критической информационной инфраструктуры РФ** (далее – критическая информационная инфраструктура);
2. **противодействия иностранным техническим разведкам на территории РФ** (далее – противодействие техническим разведкам);
3. **обеспечения защиты (некриптографическими методами) информации**.
4. **обеспечение защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;**
5. **осуществления экспортного контроля.**

Федеральный закон от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности»

Деятельность органов ФСБ осуществляется по следующим основным направлениям:

-…

- **Обеспечение информационной безопасности.**

- **Приказ ФСТЭК от 06.12.2017 г. № 227** «Об утверждении порядка ведения реестра значимых объектов КИИ»
- **Приказ ФСТЭК от 21.12.2017 г. № 235** «Об утверждении **Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования**»;
- **Приказ ФСТЭК от 25.12.2017 г. № 239** «Об утверждении **Требований по обеспечению безопасности значимых объектов КИИ РФ**;
- **Приказ ФСТЭК от 03.04.2018 г. № 55** «Об утверждении **Положения о системе сертификации средств защиты информации**»;
- **Приказ ФСТЭК от 02.06.2020 г. № 76** «Об утверждении **Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий**».
- **Приказ ФСТЭК от 14.03.2014 г. № 31** (в ред. Приказов ФСТЭК России от 23.03.2017 № 49, от 09.08.2018 № 138) «Об утверждении **требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах**, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;
- **Приказ ФСТЭК от 15.03.2021 г. № 46** «О внесении изменений в **Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах**, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31»;
- **Приказ ФСТЭК от 10.02.2022 г. № 26** «О внесении изменений в порядок РФ, утверждённый Приказом Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 года № 227»

- ISA-TR99.00.01-2007, Технологии безопасности для систем промышленной автоматизации и управления
- ISA-62443-1-1-2007, Безопасность промышленных систем автоматизации и управления, часть 1-1: Терминология, концепции и модели
- ISA-62443-2-1-2009, Безопасность промышленных систем автоматизации и управления, Часть 2-1: Создание программы безопасности систем промышленной автоматизации и управления
- ISA-TR62443-2-3-2015, Безопасность промышленных систем автоматизации и управления, часть 2-3: Управление исправлениями в среде IACS
- ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 CSV, Безопасность систем промышленной автоматизации и управления, часть 2-4: Требования к программе безопасности для поставщиков услуг IACS (IEC 62443-2-
4:2015+AMD1:2017 CSV, IDT)
- ANSI/ISA-62443-3-2-2020, Безопасность промышленных систем автоматизации и управления, Часть 3-2: Оценка риска безопасности при проектировании системы
- ANSI/ISA-62443-3-3-2013, Безопасность промышленных систем автоматизации и управления, Часть 3-3: Требования к безопасности системы и уровни безопасности
- ANSI/ISA-62443-4-1-2018, Безопасность промышленных систем автоматизации и управления, Часть 4-1: Требования к жизненному циклу разработки безопасных продуктов.
- ANSI/ISA-62443-4-2-2018, Безопасность промышленных систем автоматизации и управления, Часть 4-2: Технические требования безопасности для компонентов IACS
- Специальная публикация NIST NIST SP 800-82r3 Руководство по безопасности операционных технологий

1а. С 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), **не могут осуществлять закупки** (по 223-ФЗ) без согласования с федеральным органом исполнительной власти, уполномоченным Правительством РФ:

- **иностранного ПО**, в том числе **в составе ПАК**, в целях его использования **на** принадлежащих им **значимых объектах критической информационной инфраструктуры (ЗОКИИ);**
- **услуг**, необходимых для использования этого ПО на принадлежащих им **ЗОКИИ.**

1б. С 1 января 2025 г. органам государственной власти, **заказчикам запрещается использование иностранного ПО** на принадлежащих им **ЗОКИИ.**

2б. В 6-месячный срок реализовать комплекс мероприятий, направленных на обеспечение преимущественного применения субъектами КИИ отечественных радиоэлектронной продукции и телекоммуникационного оборудования на принадлежащих им ЗОКИИ, в том числе:

- **определить сроки и порядок перехода субъектов КИИ** на **преимущественное применение доверенных программно-аппаратных комплексов** на принадлежащих им ЗОКИИ;
- обеспечить создание и организацию деятельности научно-производственного объединения, специализирующегося на разработке, производстве, технической поддержке и сервисном обслуживании доверенных программно-аппаратных комплексов для КИИ;

6. Установить, что **с 1 января 2025 г.** органам (организациям) **запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие** в отношении РФ, российских юридических лиц и физических лиц **недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств**, прямо или косвенно подконтрольные им либо аффилированные с ними.

Постановление Правительства РФ № 2461 от 28 декабря 2022 г. **«О внесении изменений в Постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 и** признании утратившими силу отдельных положений некоторых актов Правительства Российской Федерации» **ввело** в законодательство РФ **юридически значимое определение термина ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС (ПАК)**:

ПАК – это комплекс технических и программных средств (программного обеспечения), работающих совместно для выполнения одной или нескольких специальных задач, являющийся электронной вычислительной машиной или специализированным электронным устройством (устройствами), функционально-технические характеристики которого (которых) определяются исключительно совокупностью программного обеспечения и технических средств, и не могут быть реализованы при их разделении. ПАК является самостоятельно используемым, законченным техническим изделием, имеющим серийный номер.

С вводом данного юридически значимого определения термин **программно- аппаратный комплекс (ПАК),** введенный Указом Президента № 166 получил **однозначное толкование,** а его **«ДОВЕРЕННОСТЬ»** определяется Приказом ФСТЭК № 76 от 02.06.2020 г.

28 декабря 2023 года Приказом № 115-пнст Федерального агентства по техническому регулированию и метрологии «Об утверждении предварительного национального стандарта Российской Федерации» утвержден предварительный **национальный стандарт РФ ПНСТ 905-2023 «Критическая информационная инфраструктура. Доверенные программно-аппаратные комплексы. Термины и определения» с датой введения в действие 1** ***апреля 2024 года и сроком до 1 апреля 2027 г.***

При выполнении различных работ, выполнении НИОКР применительно к системам технологического управления в составе объектов КИИ, проектировании технических решений, составлении технических заданий и т.д**. целесообразно использовать ПНСТ-905-2023 для однозначного толкования предметной области доверенных ПАК для КИИ.**

Постановление Правительства РФ от 14.11.2023 г. № 1912 **«О порядке перехода субъектов критической информационной инфраструктуры РФ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации»** определяет ряд важных моментов для ЗОКИИ:

- Утверждает **правила перехода субъектов КИИ РФ на преимущественное применение доверенных ПАК на принадлежащих им ЗОКИИ;**
- Определяет, что **переход субъектов КИИ РФ на преимущественное применение доверенных ПАК на принадлежащих им значимых объектах КИИ РФ осуществляется до 1 января 2030 г.;**
- **Не допускается с 1 сентября 2024 г. использование субъектами КИИ РФ** на принадлежащих им **ЗОКИИ ПАК**, **приобретенных субъектами КИИ РФ с 1 сентября 2024 г. и не являющихся доверенными программно-аппаратными комплексами**, за исключением случаев отсутствия произведенных в РФ доверенных ПАК, являющихся аналогами приобретенных субъектами КИИ РФ ПАК;
- Утверждает, что **доля доверенных ПАК на ЗОКИИ** по состоянию **на 31 декабря 2029 г.** должна составлять **100 процентов** в общем количестве ПАК на ЗОКИИ;
- Вводит **критерии доверенного ПАК для ЗОКИИ.**

Отраслевые документы по ИБ объектов электроэнергетики (ОКИИ)

Название	
Положение ПАО «Россети» о единой технической политике в электросетевом комплексе	Решение Совета директоров ПАО «Россети», протокол заседания от 28.12.2024 № 673
Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса группы компаний «Россети»	Распоряжение ПАО «Россети» № 282р от 30.05.2017 г.
Об утверждении требований по обеспечению безопасности информации микропроцессорных устройств релейной защиты и автоматики	Распоряжение ПАО «Россети» № 62р от 28.02.2022 г.
Методика проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе	Приказ ПАО «Россети» № 391 от 28.08.2020 г.
СТО 34.01-21-004-2019 ПАО «Россети» «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110–220 кВ и узловых цифровых подстанций напряжением 35 кВ»	Приказ ПАО «Россети» № 64 29.03.2019 г.
СТО 34.01-21-005-2019 ПАО «Россети» «Цифровая электрическая сеть. Требования к проектированию цифровых распределительных электрических сетей 0,4-220 кВ»	Приказ ПАО «Россети» № 64 29.03.2019 г.
СТО 56947007-29.240.10.256-2018 «Технические требования к аппаратно-программным средствам и электротехническому оборудованию ЦПС»	Приказ ПАО «Россети» № 355 от 21.09.2018 г.
Документ «ПЕРЕЧЕНЬ ТИПОВЫХ ОТРАСЛЕВЫХ ОБЪЕКТОВ КИИ, ФУНКЦИОНИРУЮЩИХ В СФЕРЕ ЭНЕРГЕТИКИ» (https://minenergo.gov.ru/opendata/7715847529-perechen-obektov-kii-2023)	Рекомендации Министерства энергетики РФ, Первичная публикация 08.08.2023 г.

Передача ЭЭ и технологическое присоединение к распределительным электросетям и деятельность по распределению энергии

Отраслевые объекты КИИ	Осуществляемые критические процессы типовым отраслевым объектом КИИ
Системы, предназначенные для управления сбором и передачей информации подстанции	**Сбор (измерение), первичная обработка, контроль и регистрация текущей аналоговой информации о режимных параметрах электрической сети. Сбор, обработка, контроль и регистрация текущей дискретной информации о состоянии схемы соединений и оборудования энергообъекта. Оперативный контроль и визуализация текущего режима и состояния оборудования энергообъекта на мнемосхеме. Синхронизация времени всех устройств, входящих в состав системы, с точностью до 1 мс. Обмен информацией с центрами управления с использованием стандартных протоколов...**
Системы для диспетчерского и технологического управления электрическими сетями	**Сбор и выдача информации для устройств телемеханики. Контроль исправности устройств телемеханики и каналообразующей аппаратуры. Масштабирование и контроль достоверности телеизмерений. Дорасчет нетелеизмеряемых режимных параметров. Обработка и достоверизация контрольных замеров нагрузок. Прогноз нагрузок в узлах электрических сетей на характерные периоды. Телеуправление, контроль и представление сетей. Дорасчет и контроль параметров режима.** Накопление данных реального времени, суточная ведомость. **Оценка состояния электрической сети.** Формирование и контроль баланса мощности и энергии. Оперативный расчёт и оптимизация режима распределительной сети, расчёт потерь мощности и энергии. Расчет режимов сетей. **Сбор информации с локальных систем управления. Контроль работоспособности оборудования и каналов связи.** …

- Нормативная база сложилась и в развитии;
- Техническая (СЗИ) база сложилась;
- Значимый объект КИИ РФ – сфера компетенции ФСТЭК России и ФСБ России.

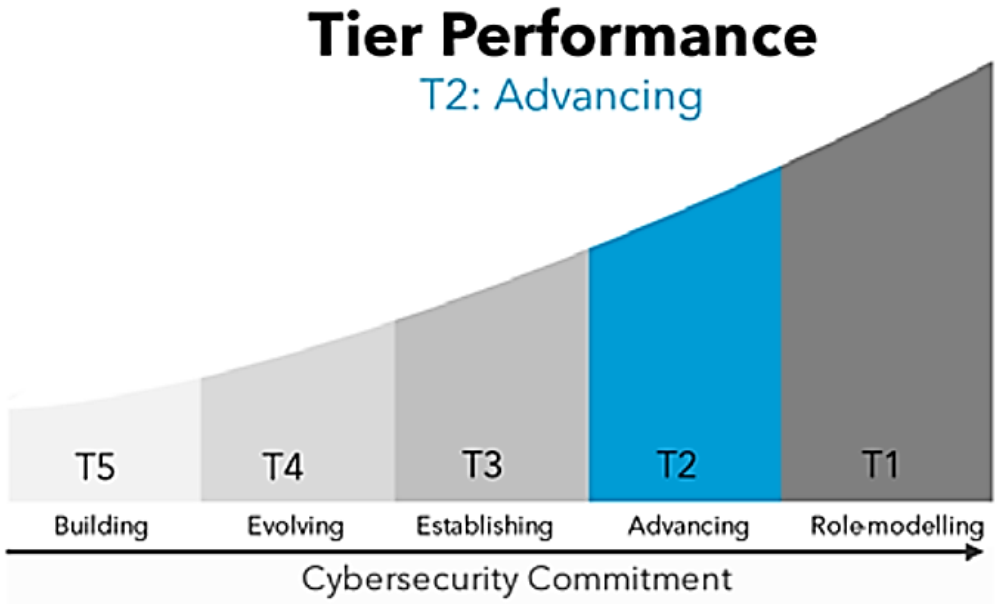
Международный индекс кибербезопасности РФ (Канада, Китай, Израиль, Швейцария**) – прогрессирующий**

Оценка уровня кибербезопасности РФ по пяти направлениям: правовые, технические и организационные аспекты, развитие потенциала, а также уровень сотрудничества

Country Score
out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures
20	16.59	20	18.77	16.77

Максимальные баллы в правовой и организационной плоскостях.



https://ict.moscow/research/global-cybersecurity-index-2024/

Международный союз электросвязи (МСЭ, ITU)

2. ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ ПРИ УПРАВЛЕНИИ ЭЭС

Системы SCADA и СМПР являются **наиболее уязвимыми** к кибератакам в ИС. Поскольку **система управления** влияет на ЭЭС через **управляющие воздействия** или свои выходные данные, то **последствия**, вызванные реализованными киберугрозами в этих системах, представляют **наибольшую опасность для функционирования ЭЭС.**

Надежное функционирование ЭЭС зависит от применяемых информационных и коммуникационных технологий в цифровых системах управления. В условиях цифровизации ЭЭС становится более уязвимой к информационным сбоям и кибер-инцидентам в ИС.

КА на **систему SCADA и СМПР** могут привести **к выработке и реализации неправильных управляющих воздействий и к развитию аварийных ситуаций в ЭЭС** (рис. 2.1).

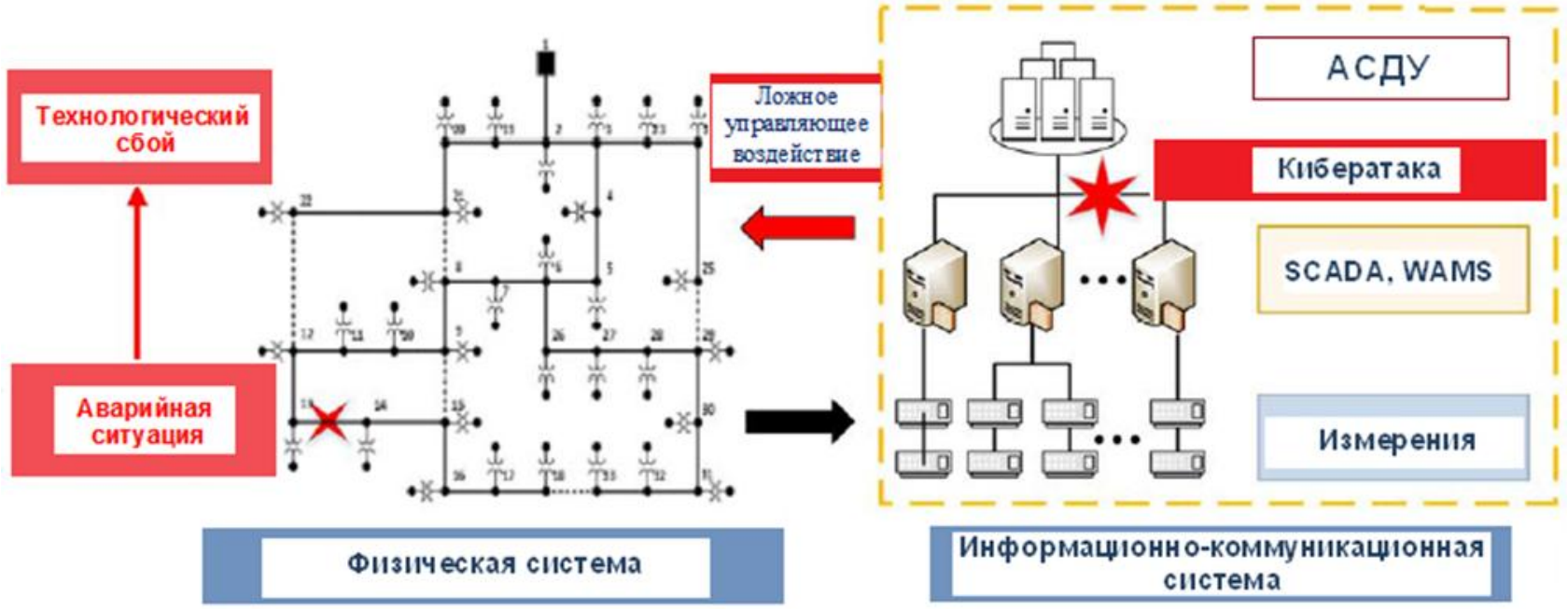


Рис. 2.1. Влияние ложных управляющих воздействий на функционирование ЭЭС

Таблица 2.1. Влияние кибератак на функции управления и связанные с ними последствия для ЭЭС

Угрозы	ИКИ	Система управления	Физическая система
Атаки внедрения ложных данных	SCADA (RTU), СМПР (PMU, PDC), ПВК «Оценка», EMS, DMS	Выработка неправильных УВ. Потеря контроля частоты, напряжения. Потеря наблюдаемости. Неправильные диспетчерские команды. Ложные характеристики нарушений окажет влияние на операции распределения и передачи.	Нарушение устойчивости Большие колебания в динамике системы: отключение доп. линий; отключение генераторов; сброс нагрузки. Блэкаут.
Атаки синхронизации времени (spoofing-атаки и др.)	СМПР (PMU, каналы связи между PMU и PDC, GPS), ПВК «Оценка»	Ложная визуализация текущего режима, что приводит к ошибочным действиям по контролю и защите. Потеря контроля частоты, напряжения. Ложная информация о наличии и места неисправности. Рассогласование команд на отключение/срабатывание ИУ.	Вызывает отключение линии электропередачи, затем может вызвать каскадную цепочку аварий в системе. Нарушение устойчивости.
Атаки отказа в обслуживании (DoS-, jamming-атаки и др.)	SCADA (RTU), СМПР (PMU, PDC), ПВК «Оценка», EMS, DMS	Задержка управления. Выработка неправильных УВ. Потеря контроля частоты, напряжения. Блокировка управляющего сигнала. Потеря наблюдаемости.	Нарушение устойчивости. Увеличение времени восстановления системы. Нарушение баланса генерация-нагрузка. Отказ отключения/ срабатывания ИУ.
Атаки динамической системы (DDoS)	SCADA (RTU), СМПР (PMU, PDC), ПВК «Оценка»	Задержка управления. Потеря наблюдаемости. Нарушение контроля частоты, напряжения.	Нарушение устойчивости.
Скоординированные атаки	SCADA (RTU), СМПР (PMU), ПВК «Оценка»	Все перечисленное выше.	Нарушение устойчивости. Каскадные аварии в системе.
Вредоносное ПО (Backdoor, worms, Trojan hors)	SCADA (HMI), СМПР	Некорректная выработка УВ. Неправильное срабатывание аппаратных и программных устройств. Потеря контроля частоты, напряжения.	Нежелательное отключение/срабатывание ИУ. Нарушение устойчивости. Коллапс напряжения. Блэкаут.

Риск – это вероятность нежелательного исхода в результате инцидента, события или нарушения, определяемая его вероятностью и связанными с этим последствиями (нанесенным ущербом). **Риск** представляет собой **комбинацию вероятности реализации угрозы** и **последствий** (ущерба) от нее в отношении защищаемого актива (ресурса). **Последствия** определяются уровнем воздействия. При оценке рисков при управлении ЭЭС в качестве **актива** рассмотрены **системы SCADA и СМПР**, **потеря управления** – нанесенный **ущерб** реализованной КА, влекущий за собой неблагоприятные последствия для функционирования ЭЭС.

Этапы оценки риска

1. Оценка риска кибербезопасности при каждой реализованной киберугрозе;
2. Определение результирующей оценки риска.

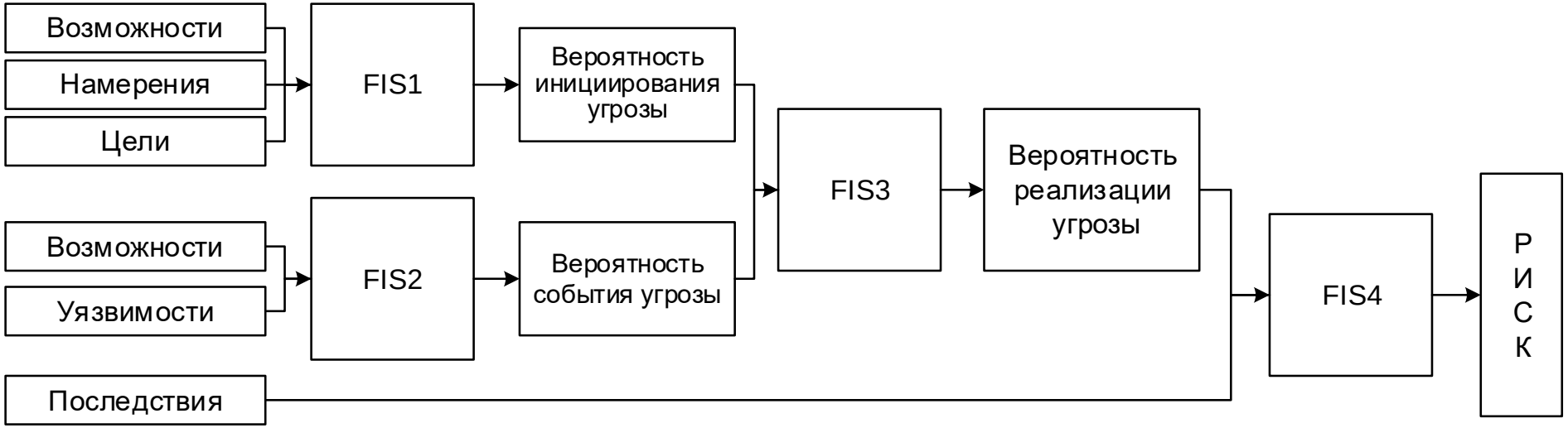


Рис. 2.2. Иерархическая система оценки рисков кибербезопасности цифровой системы управления

Результирующая оценка риска кибербезопасности цифровой системы управления R_C определяется как сумма оценок рисков R_{ci} при i-й КА – $R_C = \sum_{i=1}^{n} R_{ci}$.

Для оценки риска при управления ЭЭС рассмотрены реализации jamming-атаки (тип DOS-атаки) и spoofing-атаки (тип синхронизированной атаки) на систему СМПР.

Таблица 2.2. Входные факторы риска

	Jamming-атака	**Spoofing-атака**
Возможности	0,75	0,97
Намерения	0,76	0,92
Цели	0,6	0,7
Уязвимости	0,85	0,92
Последствия	0,92	0,93

Таблица 2.3. Выходные факторы риска

	Jamming-атака	**Spoofing-атака**
Вероятность инициирования угрозы	0,63	0,81
Вероятность события угрозы	0,76	0,81
Вероятность реализации угрозы	0,69	0,75
Риск	0,67 – средний уровень	0,72 – средний уровень

Результирующая оценка риска ***Rc=0,91*** говорит о **высоком уровне риска** и позволяет сделать выводы, что успешное совместное проведение jamming-атаки и spoofing-атаки может нанести гораздо больший урон электроэнергетической системе и вызвать серьезные последствия в ее работе, чем при реализации каждой КА по отдельности.

В отсутствие устоявшейся нормативной базы, предложенная методика оценки рисков кибербезопасности позволяет определить наиболее уязвимые цифровые объекты ЭЭС, уровень их защищенности, оценить последствия реализованных кибератак на цифровые объекты ЭЭС.

Поскольку оценка рисков кибербезопасности основана на вероятностных моделях угроз и нарушителей, применение данной методики целесообразно и при разработке комплекса организационных и технических мероприятий по снижению влияния киберугроз на цифровые объекты ЭЭС.

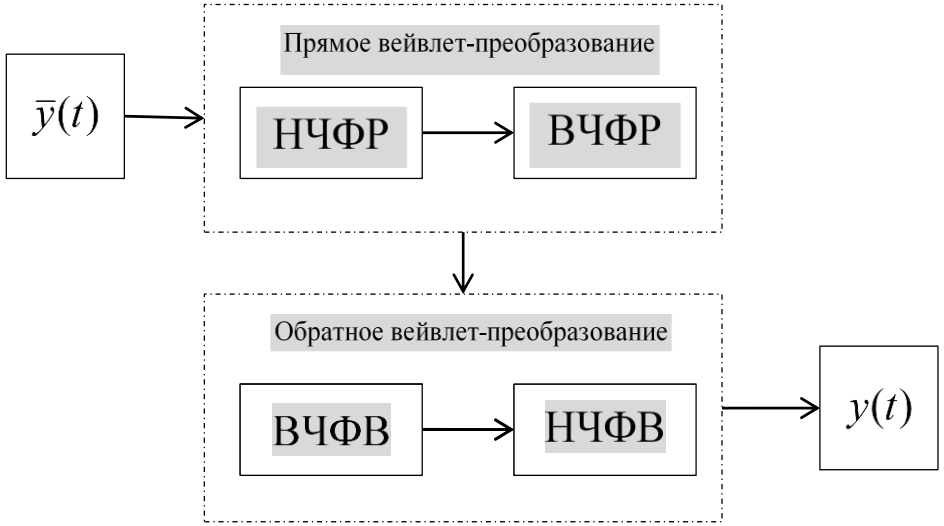
3. МЕТОДЫ ПОВЫШЕНИЯ КАЧЕСТВА ИНФОРМАЦИИ ПРИ УПРАВЛЕНИИ ЭЭС В УСЛОВИЯХ КИБЕРАТАК

Модель измерения параметров режима при наличии недостоверных данных, появившихся в результате КА

$$\bar{y}(t) = y(t) + \xi_y(t) + a(t), \qquad (3.1)$$

$y(t)$ - поток истинных значений измеряемых параметров; $\xi_y(t)$ - вектор шума измерений, имеющий нормальное распределение
$\xi_y \to N(0, \sigma_y^2)$ с нулевым математическим ожиданием и дисперсией σ_y^2, характеризующей точность измерений; $a(t)$ - кибератака.

Алгоритм достоверизации данных на основе вейвлет-анализа



Достоинством применения вейвлет-преобразований потоков измерений является снижение влияния кибератак на достоверность информации путем фильтрации шумов и удаления (сглаживания) ошибок в измерениях.

Вейвлет-анализ информационных потоков состоит из прямого вейвлет-преобразования (ПВП) и обратного вейвлет-преобразования (ОВП). ПВП состоит в разложении сигнала на **аппроксимирующие коэффициенты** $A = \{A_k\}$, представляющие собой сглаженный процесс, и **детализирующие коэффициенты** $D = \{D_k\}$, описывающие колебания, с последующим их уточнением итерационным методом, как во временной, так и в частотной областях.

Атаки внедрения ложных данных

$KA1$ – дополнительный шум $a(t) = \xi_{\text{КА1}}(t) \to N(0, \sigma_y^2)$, $\sigma_a^2 > \sigma_y^2$. $\bar{y}(t) = y(t) + \xi_y(t) + \xi_{\text{КА1}}(t)$.

$KA2$ – дополнительные ошибки $a(t) = b_{\text{КА2}}$, $\bar{y}(t) = y(t) + \xi_y(t) + b_{\text{КА2}}(t)$.

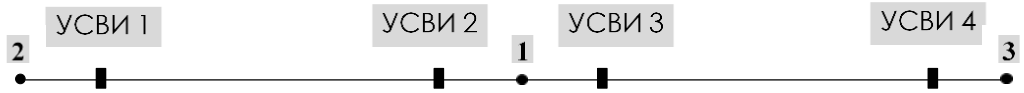
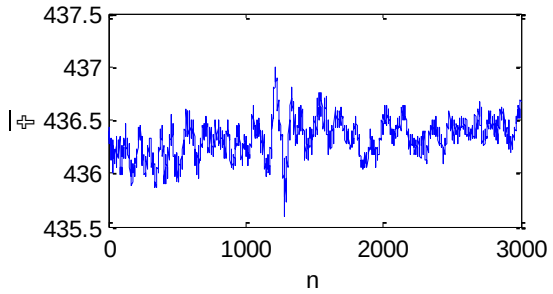
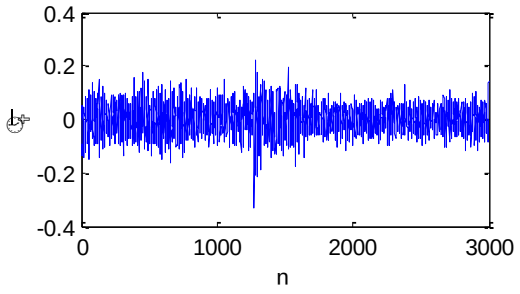


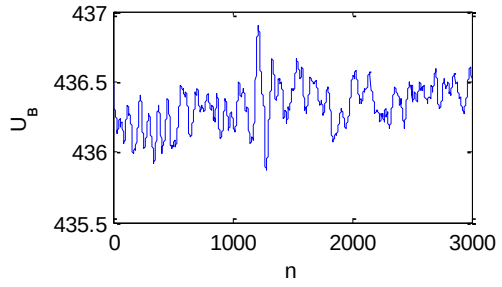
Рис. 3.1. Схема участка электрической сети



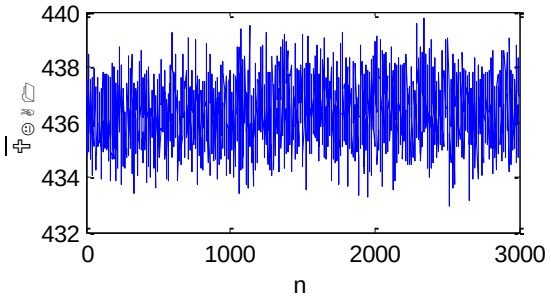
а) Измерение напряжения $\overline{U}$, кВ



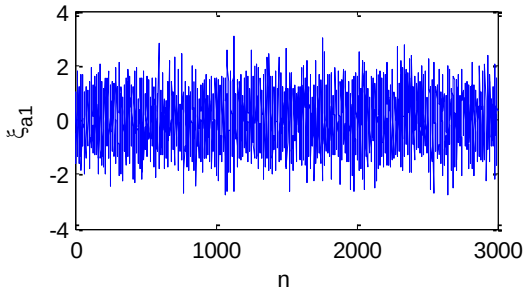
в) Шум измерения, $\xi_{\overline{U}}$



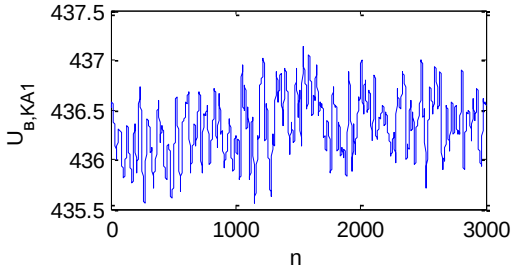
д) Напряжение $U_в$, кВ



б) Измерение напряжения $\overline{U}_{KA1}$, кВ

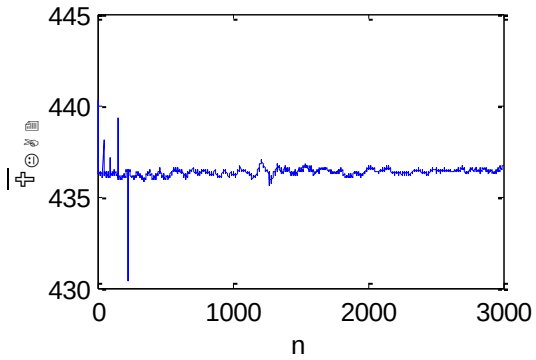


г) Шум измерения при $KA1$, ξ_{a1}

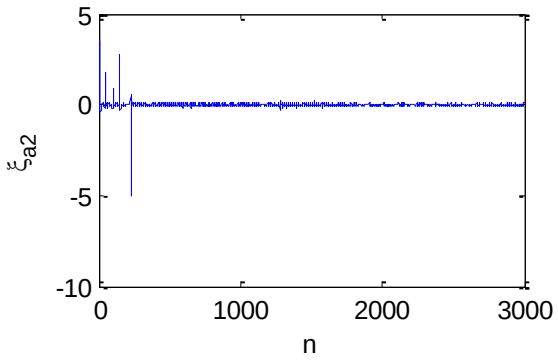


е) Напряжение $U_{в,KA1}$, кВ

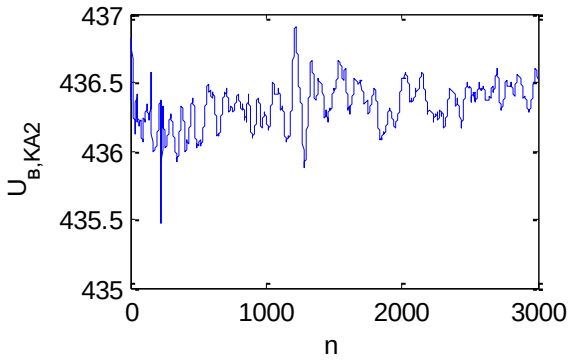
Рис. 3.2. Восстановление качества данных при кибератаке *КА1*



а)Измерение напряжения $\overline{U}_{\text{КА2}}$, кВ



б) Шум измерения при КА2



в) Восстановленное напряжение $U_{\text{в,КА2}}$, кВ

Рис. 3.3. Восстановление качества данных при кибератаке *КА2*

Таблица 3.1. Сравнительный анализ характеристик исходных данных и данных при кибератаках, полученных в результате достоверизации синхронизированных векторных измерений

	$y(t)$	КА1	$\xi_{\overline{U}} = \xi_y$	$\xi_{a1} = \xi_{\overline{U}} + \xi_{\text{КА1}}$	КА2	
	$U_{\text{в}}$, кВ	$U_{\text{в,КА1}}$, кВ	$\xi_{\overline{U}}$	ξ_{a1}	$\overline{U}_{\text{КА2}}$, кВ	$U_{\text{в,КА2}}$, кВ
Математическое ожидание, m	436,3	436,3	$1{,}841 \cdot 10^{-13}$	$1{,}795 \cdot 10^{-13}$	436,3	436,3
СКО, σ	0,1593	0,3058	0,04919	0,9056	0,2234	0,1622
Минимальное значение, min	435,9	435,6	-0,3335	-2,75	430,4	435,5
Максимальное значение, max	436,9	437,1	0,2226	3,06	440,3	436,9

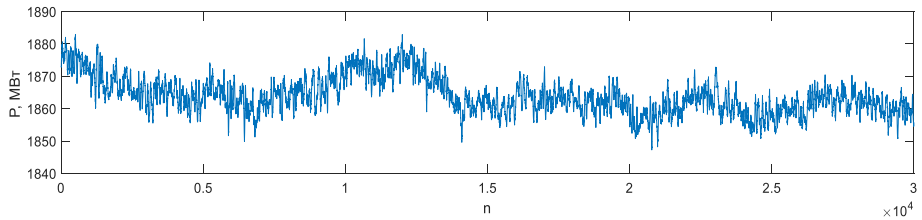


Рис. 3.4. Изменение перетока активной мощности $P_{2\text{-}3}$

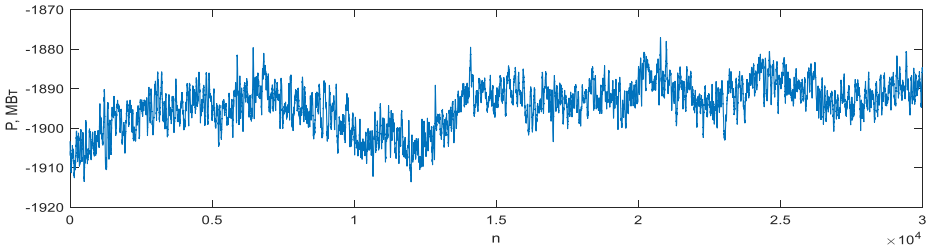


Рис. 3.5. Изменение перетока активной мощности $P_{3\text{-}2}$

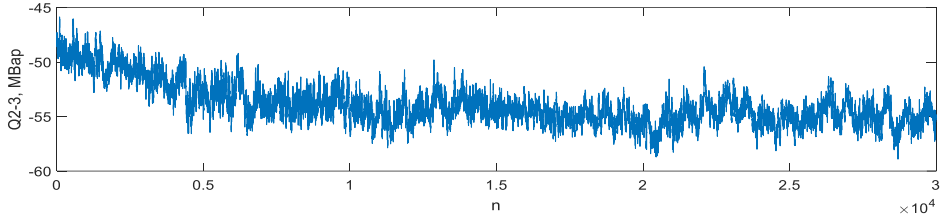


Рис. 3.6. Изменение перетока реактивной мощности $Q_{2\text{-}3}$

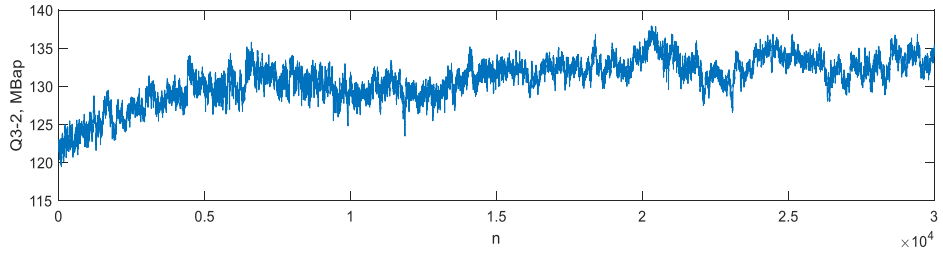


Рис. 3.7. Изменение перетока реактивной мощности $Q_{3\text{-}2}$

Моделирование случайных ошибок измерений проводилось на эталонном установившемся режиме, полученным расчетным путем по программе расчета установившегося режима или ОС.

Расчеты при моделировании FDI-атак, не идентифицируемых традиционными методами ОПД:

- **метод КУ**, когда проверка достоверности измерений выполняется по невязкам КУ;
- **классический метод ОС**, когда проверка достоверности измерений выполняется по взвешенным остаткам оценивания.

Модель измерений при FDI-атаке в виде ошибок $b_{\text{КА}}$:

$$\bar{y}(t) = y(t) + \xi_y(t) + b_{\text{КА}}(t) \qquad (3.2)$$

Таблица 3.2. Характеристики процессов изменения перетоков активной мощности и реактивной мощности линии 2-3, требуемые при построении системы логического вывода

	P_{2-3}	P_{3-2}	Q_{2-3}	Q_{3-2}
m_y	-1864	1894	-53.94	130.9
σ_y	5.635	5.772	1.896	2.826
min_y	-1883	1877	-58.9	119.5
max_y	-1847	1914	-45.86	137.9

Для проверки достоверности измерений методом КУ формируются контрольные уравнения и проверяется условие: $\lfloor w_k \rfloor \leq d_k$ (3.3)

где w_k - невязка КУ, d_k - некоторое пороговое значение.

Если условие (3.3) выполняется, то все измерения в данном КУ считаются **достоверными.**

Таблица 3.3. Результаты ОС по методу КУ и идентификации ошибочных измерение методом ОПД и BDId

Параметр	Эталон	Без ошибки	С грубой ошибкой	метод КУ		BDId
				ОПД	ОС	
P_{1-2}	-992,7	-993	--	дост	-994	дост
Q_{1-2}	-187,5	-183	--	дост	-189	дост
P_{2-1}	1010	1013	-	дост	1011	дост
Q_{2-1}	-468	-446	-	дост	-464	дост
P_{2-3}	**-1880**	**-1879**	**-1979**	**дост**	**1982**	**ошиб**
Q_{2-3}	29	34	-	дост	48	дост
P_{3-2}	**1896**	**1903**	**2003**	**дост**	**2000**	**ошиб**
Q_{3-2}	-92	-90	-	дост	-85	дост
Значение целевой функции – 9,98						

Искаженные измерения методом КУ определялись как достоверные и использовались алгоритмом ОС для расчета оцененного режима. Полученные оценки существенно отклоняются от эталонного режима, хотя значение целевой функции удовлетворяет χ-квадрат критерию.

Анализ измерений P_{2-3} и P_{3-2} на основе алгоритма BDId позволил идентифицировать измерения как ошибочные с уровнем точности, равным 0,12 (низкий уровень).

Задача ОС решается классическим методом через вектор состояния x, а ОПД выполняется после ее решения (апостериорно) по взвешенным остаткам оценивания, которые для достоверных измерений не должны превышать величину порога, равную 3-3.5.

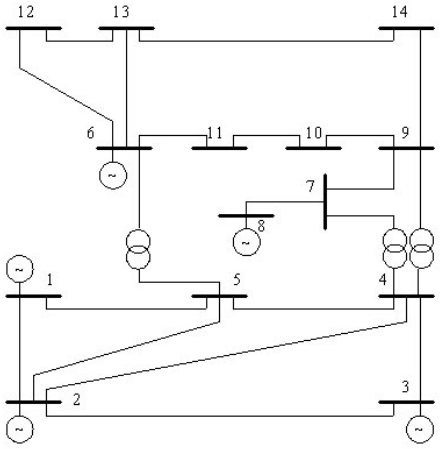
Таблица 3.4. Результаты ОС классическим методом, идентификация ошибочных измерений по взвешенным отстаткам и BDId

Параметр	Эталон	Без грубой ошибки	Атака	С грубой ошибкой	Расчет классическим методом		BDId
					ОС	Взвеш. остатки	
P_{1-2}	-992,7	-993	0	-	-994	0,256	
Q_{1-2}	-187,5	-183	0	-	-189	0,709	
P_{2-1}	1010	1013	0	-	1011	0,257	
Q_{2-1}	-468	-446	0	-	-464	1,86	
P_{2-3}	**-1880**	**-1879**	**-32,5**	**-1911**	**-1928**	**3,49**	**ошиб**
Q_{2-3}	**29**	**34**	**-432,5**	**-398**	**-395**	**0,327**	**ошиб**
P_{3-2}	**1896**	**1903**	**33,3**	**1963**	**1946**	**3,05**	**ошиб**
Q_{3-2}	**-92**	**-90**	**434,8**	**345**	**339**	**0,682**	**ошиб**
Значение целевой функции 20,17							

Полученные результаты свидетельствуют о том, что, несмотря на внесенные в вектор состояния искажения, метод анализа взвешенных остатков не обнаружил ошибочных измерений. На основе алгоритма BDId вычисленные уровни точности для $P_{2\text{-}3}$ (0.126), $Q_{2\text{-}3}$ (0.117), $P_{3\text{-}2}$ (0.125), $Q_{3\text{-}2}$ (0.117), позволили идентифицировать эти измерения как ошибочные.

Пример. Оценивание состояния ЭЭС при DOS-атаках на систему SCADA методом внутренней точки

Рассмотрена 14-узловая тестовая схема IEEE. В каждом узле установлено устройство RTU.



Предположим, что в результате DoS-атаки на систему SCADA произошла потеря измерений RTU второго узла: P_2, Q_2, P_{2-1}, P_{2-3}, Q_{2-3}, P_{2-4}, Q_{2-4}, P_{2-5}, Q_{2-5}, которые образуют вектор z. Вектор y составили измерения P_1, Q_1, U_1, P_4, Q_4, P_5, Q_5, U_5, P_{11}, Q_{11}, P_{13}, Q_{13}, P_{14}, Q_{14}, P_7, Q_7, P_8, Q_8, P_3, Q_3, P_6, Q_6, P_9, Q_9, P_{10}, Q_{10}, U_{10}, P_{12}, Q_{12}, Q_{1-2}, P_{1-5}, Q_{1-5}, , P_{3-4}, Q_{3-4}, P_{4-5}, Q_{4-5}, P_{4-7}, Q_{4-7}, P_{4-9}, Q_{4-9}, P_{5-6}, Q_{5-6}, P_{6-11}, Q_{6-11}, P_{6-12}, Q_{6-12}, P_{6-13}, Q_{6-13}, P_{7-8}, Q_{7-8}, P_{7-9}, Q_{7-9}, P_{9-10}, Q_{9-10}, P_{9-14}, Q_{9-14}, P_{10-11}, Q_{10-11}, P_{13-14}, Q_{13-14}, P_{14-13}, P_{12-13}, Q_{14-13}.

Ограничений-неравенства для вектора z:

$0 \le P_2 \le 50$, $0 \le Q_2 \le 50$, $-160 \le P_{2-1} \le 0$, $0 \le P_{2-3} \le 100$, $0 \le Q_{2-3} \le 10$, $0 \le P_{2-4} \le 100$, $0 \le Q_{2-4} \le 10$, $0 \le P_{2-5} \le 100$, $0 \le Q_{2-5} \le 10$.

Ограничения для измерений напряжения:

$65.7 \le U_1 \le 80.3$, $63 \le U_5 \le 70$, $12.6 \le U_1 \le 15.4$.

Для сопоставления полученных результатов ОС с существующими методами задача также была решена в ПВК «Оценка».

Вычисленные значения критерия минимизации при ОС (рис. 3.8):

1. сумма взвешенных квадратов отклонений измерений от эталонных значений;
2. сумма взвешенных квадратов отклонений полученных оценок измерений в ПВК «Оценка» от эталонных значений при КА;
3. сумма взвешенных квадратов отклонений, полученных предложенным алгоритмом ОС оценок измеренных и неизмеренных параметров режима от эталонных значений.

Полученные результаты подтвердили требуемую точность решения задачи ОС для случая 3 и эффективность использования МВТ при потере измерений.

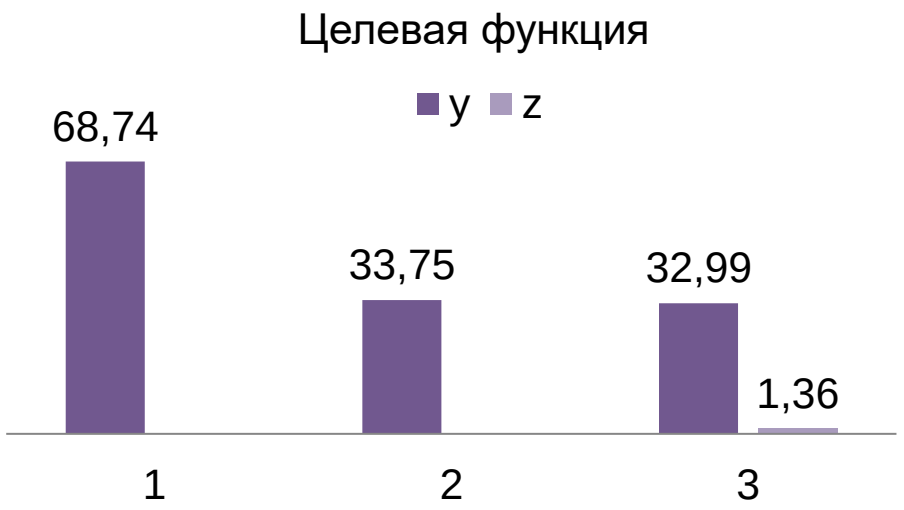


Рис.3.8. Минимизация целевой функции

При достоверизации информации целесообразно использование вейвлет-анализа, позволяющего быстро обнаруживать кибератаки и компенсировать их воздействие на цифровые системы управления ЭЭС.

Предложен алгоритм обнаружения ошибочных измерений, возникающих при кибератаках и не идентифицируемых традиционными методами достоверизации измерений при оценивании состояния ЭЭС. Использование предложенного алгоритма позволит своевременно исключить влияние успешно реализованных кибератак на результаты ОС ЭЭС, тем самым обеспечивая функции управления достоверной информацией.

Разработан подход к ОС ЭЭС на основе метода внутренней точки, позволяющий в случае потери измерений получить их оценки. Результаты расчетов показали эффективность использования предложенного подхода решения задачи ОС ЭЭС при атаке отказа в обслуживании.

4. МЕТОДИКА ОЦЕНКИ УСТОЙЧИВОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ЭЭС ПРИ КИБЕРАТАКАХ

Устойчивость - способность системы и ее составных частей предвидеть, поглощать, адаптироваться и восстанавливаться при кибератаках. Таким образом, **Устойчивость ИС ЭЭС зависит от способности противостоять негативным воздействиям** (сопротивление и поглощение), **способности восстановления и живучести, т.е. способности предотвращать нарушения функциональности при кибератаках. Возврат системы в нормальное состояние означает способность системы к адаптации и восстановлению.**

Функциональность является одним из важных показателей, используемых для оценки производительности системы с учетом ее надежности. Она определяется как способность выполнять требуемую функцию при определенных условиях в данный момент времени или в течение заданного интервала времени. Так возможные состояния цифрового устройства, зависящие от отказов составных частей, который обеспечивает выполнение заданных функций, можно описать полумарковской моделью.

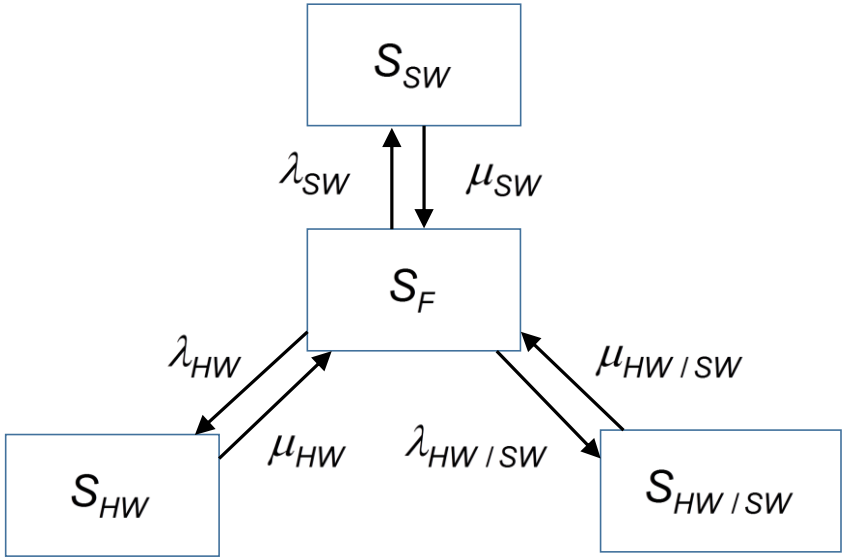


Рис 4.1. Диаграмма переходов состояний цифрового устройства ИС

S_F – полнофункциональное состояние цифрового компонента,

S_{SW} - отказ программного обеспечения,

S_{HW} - отказ аппаратного обеспечения,

$S_{HW/SW}$ - отказ взаимодействия аппаратного и программного обеспечения,

λ_{SW}, λ_{HW}, $\lambda_{HW/SW}$ - интенсивности отказов программного, аппаратного обеспечения и их взаимодействия соответственно,

μ_{SW}, μ_{HW}, $\mu_{HW/SW}$ - интенсивности восстановления программного, аппаратного обеспечения и их взаимодействия соответственно.

Для сохранения **функциональности цифрового объекта** при кибератаках на ИС ЭЭС необходимо обеспечение **более быстрых отклика и восстановления АО, ПО и их взаимодействия цифровых объектов ИС**, которые могут быть охарактеризованы **наименьшей интенсивностью отказов и максимальной интенсивностью восстановления** соответственно:

$$\lambda_i = \frac{1}{MTBF_i}, \quad (4.1)$$

$$\mu_i = \frac{1}{MTTR_i}, \quad (4.2)$$

где MTBFi - средняя наработка i-й составляющей объекта системы на отказ, MTTRi - среднее время восстановления i-й составляющей объекта системы, 1 – программное обеспечение, 2 – аппаратное обеспечение, 3 – взаимодействие аппаратного и программного обеспечения.

Уровень устойчивости цифрового объекта ИС при кибератаках можно охарактеризовать:
- **приемлемым уровнем кибербезопасности**,
- **вероятностью безотказной работы** (уровнем отклика)

$$P_{res_i} = e^{-\lambda t}. \quad (4.3)$$

- **вероятностью восстановления** (уровнем восстановления) составляющих цифрового объекта

$$P_{rec_i} = 1 - e^{-\mu t}. \quad (4.4)$$

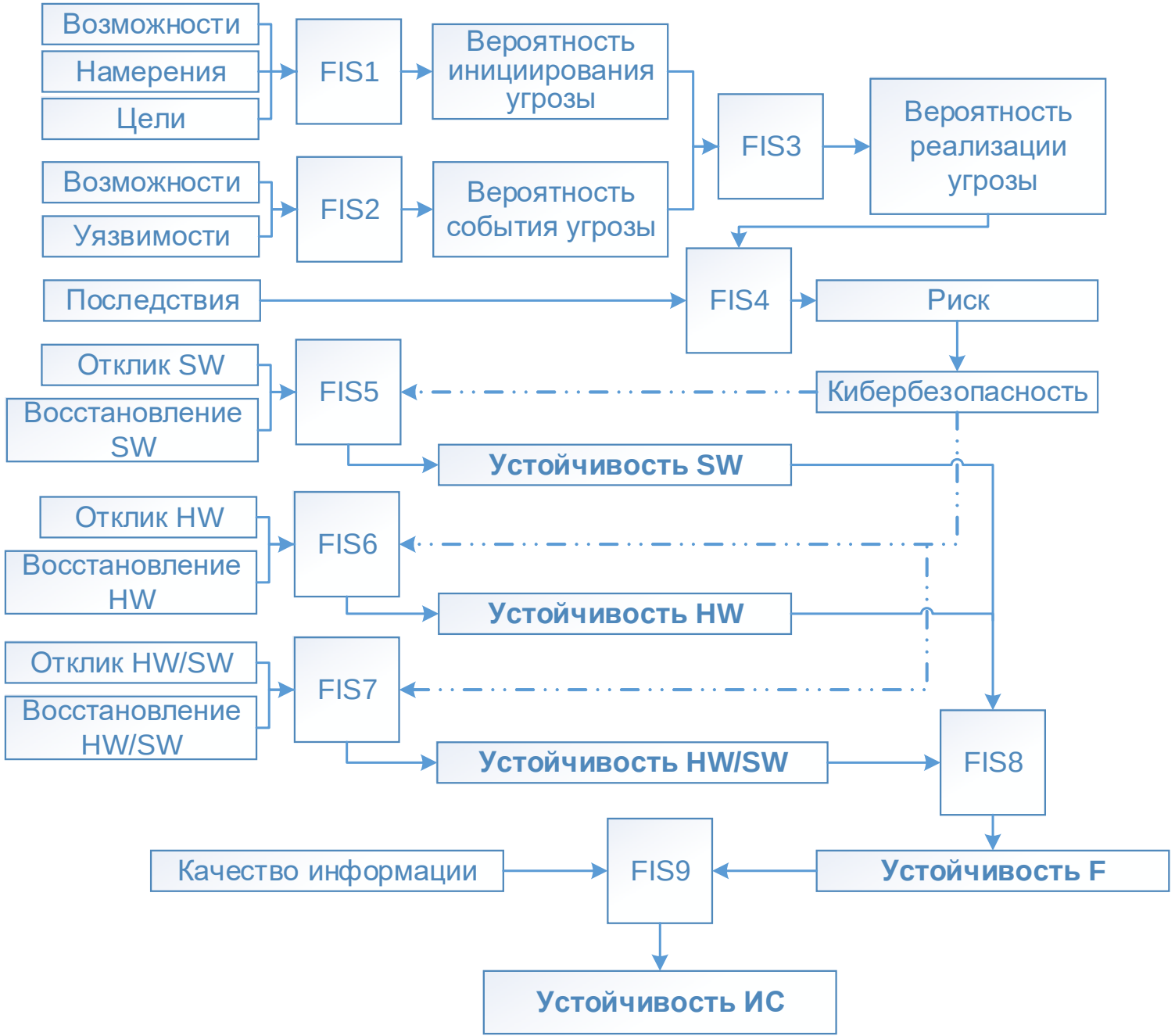


Рис. 4.2. Иерархическая система определения показателя устойчивости ИС ЭЭС при кибератаках

Пусть интервалы времени пребывания (час.) системы в каждом из состояний следующие:
$T_N = [70, 350]$; : $T_D = [20, 550]$; $T_{FP} = [5, 300]$; $T_{SD} = [5, 50]$; : $T_F = [1, 350]$.

Таблица 4.1 Факторы риска кибербезопасности ИС

Факторы риска	Вредоносное ПО
Возможности	0,6
Намерения	0,85
Цели	0,76
Уязвимости	0,75
Последствия	0,81

Таблица 4.2 Интенсивность отказа и интенсивность восстановления составляющих цифрового объекта

	λ_i	μ_i
АО	0,001	0,7
ПО	0,004	0,8
АО&ПО	0,011	0,85

Таблица 4.3 Уровни отклика и восстановления составляющих цифрового объекта

	$\tilde{R}_i^{res}$	$\tilde{R}_i^{rec}$
АО	0,99 – HL	0,99 – HL
ПО	0,96 – HL	1 – HL
АО&ПО	0,9 – HL	1 – HL

Таблица 4.4. Показатели устойчивости цифрового объекта

$\tilde{R}_1$	$\tilde{R}_2$	$\tilde{R}_3$	$\tilde{R}_{DO}$
0,86	0,9	0,9	0,89

Показатель устойчивости при нарушении доступности информации с учетом мер по восстановлению $\psi_{QI} = 0.985$.

Показатель устойчивости ИС $\tilde{R} = 0.88$.

Полученные результаты могут быть полезны при разработке мер по обеспечению устойчивости цифровых объектов информационной системы ЭЭС.

Отличительной особенностью предложенной методики является комплексный подход, позволяющий при определении показателя устойчивости учитывать оценку риска кибербезопасности, влияние качество информации и такие показатели надежности, как интенсивности отказа и восстановления цифровых объектов информационной системы при кибератаках.

Анализ состояний таких цифровых объектов, как системы управления, системы противоаварийного управления, систем сбора, обработки и передачи информации на основе предложенной методики позволит обеспечить их защищенность и более быстрое восстановление при кибератаках на ЭЭС.

5. ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ПРИ ВТОРИЧНОМ РЕГУЛИРОВАНИИ НАПРЯЖЕНИЯ В СИСТЕМАХ УПРАВЛЕНИЯ МИКРОСЕТЯМИ

1. **Моделирование взаимосвязанных микросетей.**
2. **Моделирование кибератак, оценка распространения их влияния на взаимосвязанные ИС МС.**
3. **Разработка возможных мер, обеспечивающих защищенность ИС МС от кибератак.**

Для реализации метода обнаружения и подавления последствий КА с использованием методов машинного обучения без учителя (изоляционный лес и k-ближайших соседей) и проверки его эффективности была рассмотрена система управления МС.

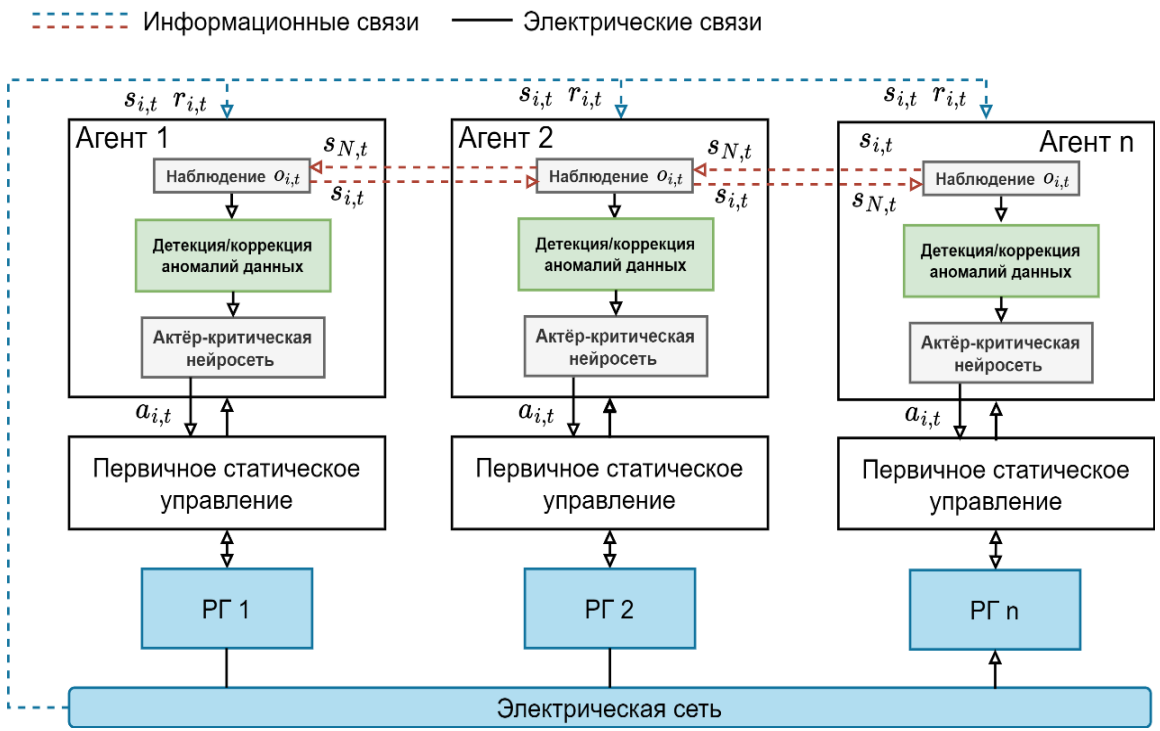


Рис. 5.1. Структура вторичного управления контроллерами инверторов с функцией защиты от КА на основе двухэтапной процедуры

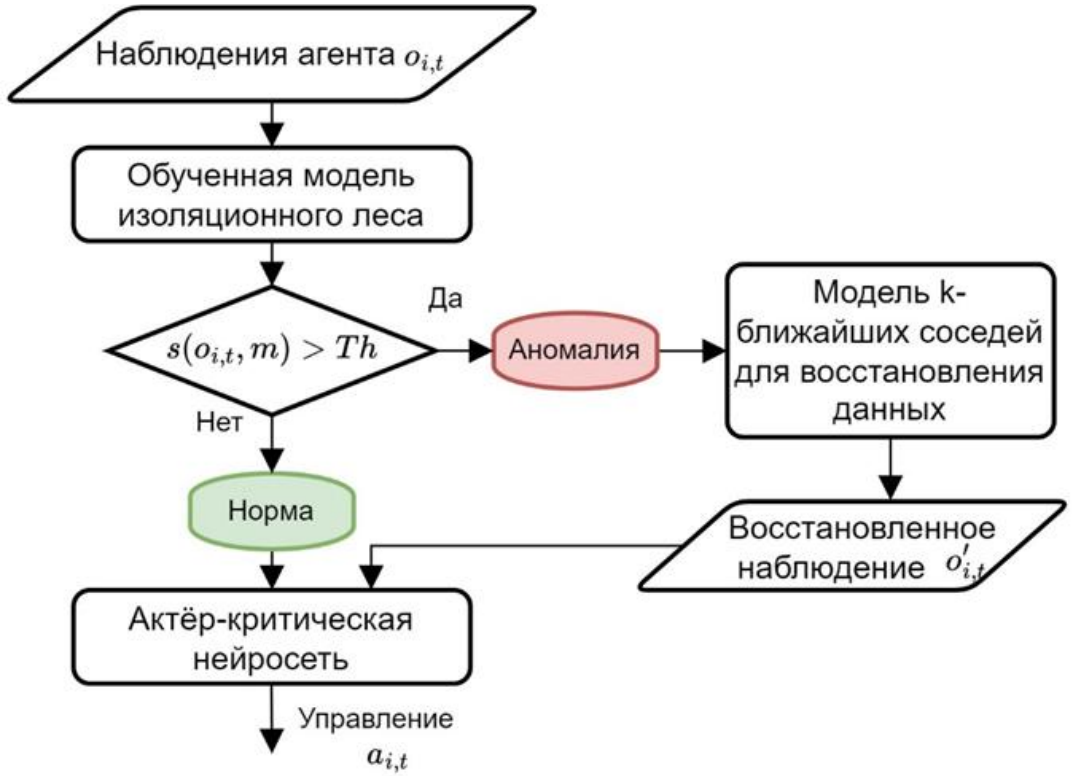


Рис. 5.2. Общая блок-схема двухэтапной процедуры обнаружения и подавления последствий КА с использованием алгоритмов МО без учителя

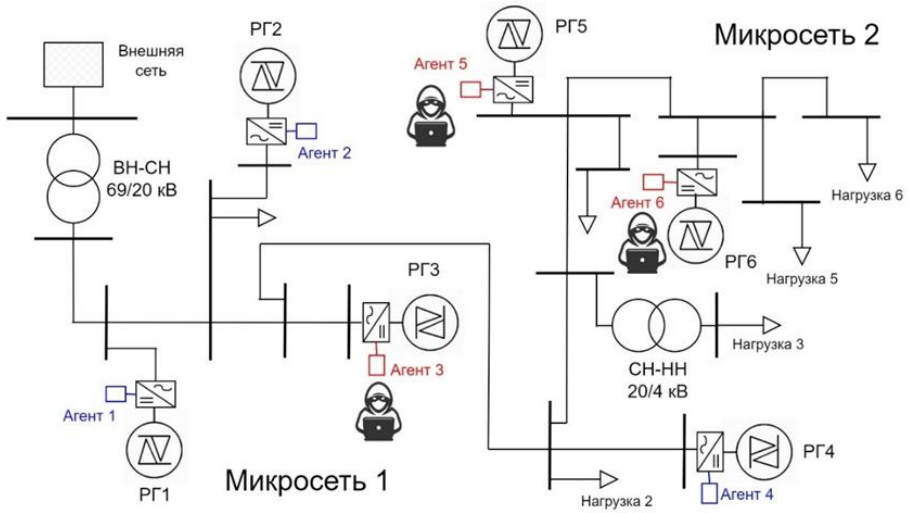


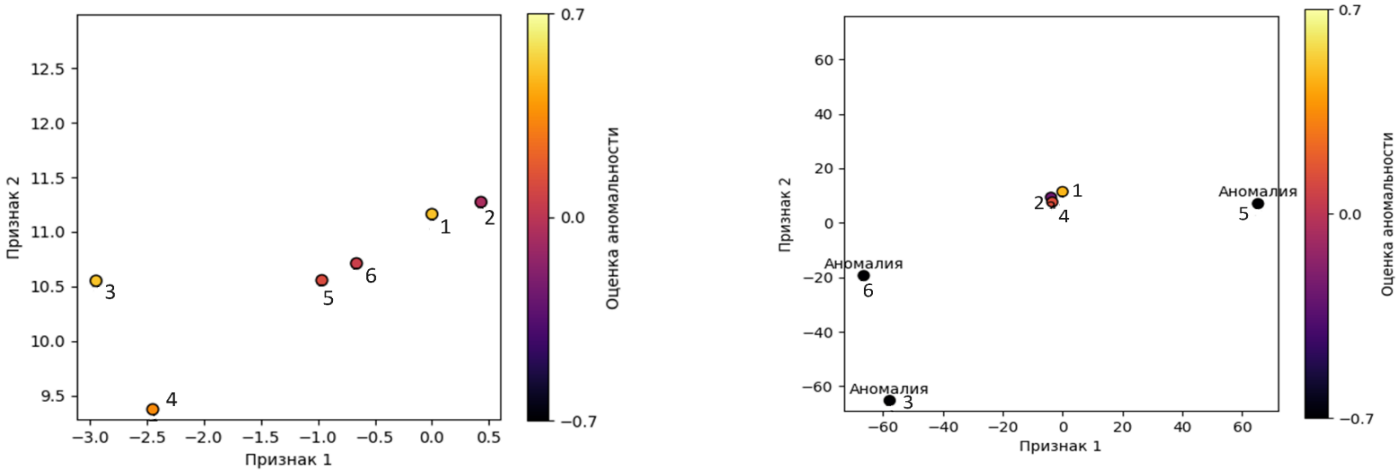
Рис. 5.3. Тестовая схема двух взаимосвязанных МС

1. **FDI-атака** $o_{i,t}^{a} = o_{i,t} - \alpha x_{i,t}^{a}$, (5.1)

где $x_{i,t}^{a}$ –ложные данные, заданные в виде случайного распределения в определённом диапазоне, $\alpha \in \{0, 1\}$ – коэффициент искажения данных, $\alpha = 1$ соответствует реализованной КА.

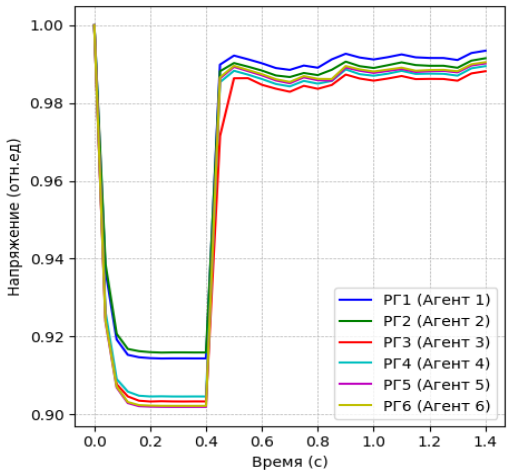
2. **Атака захвата контроллера** $o_{i,t}^{c} = (1 - \alpha) o_{i,t} - \alpha x_{i,t}^{a}$, (5.2)

где $o_{i,t}^{c}$ – модифицированные значения данных; $x_{i,t}^{a}$ –ложные данные, заданные в виде случайного распределения в определенном диапазоне, $\alpha = 1$ означает атаку на инвертор с полной заменой наблюдений.

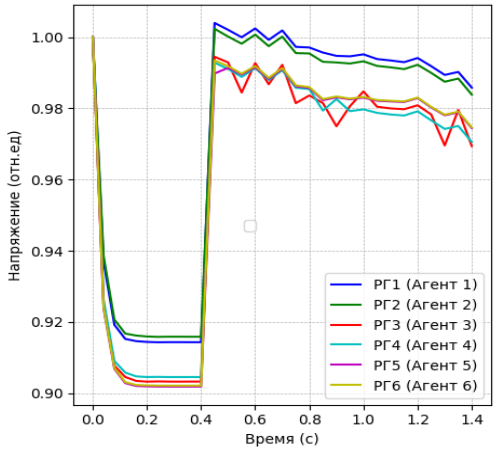


а) В отсутствие кибератаки б) Hijacking-атака

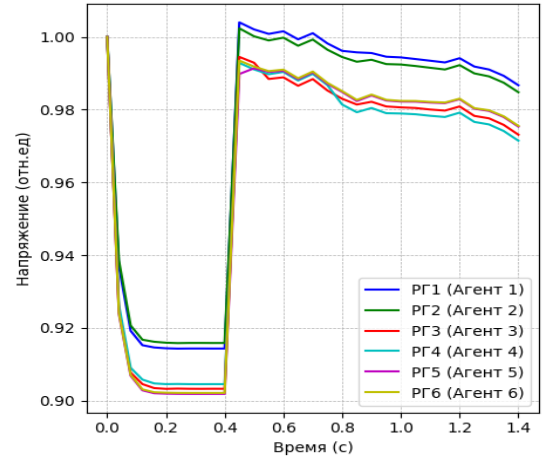
Рис. 5.4. Визуализация оценки векторов наблюдений агентов при аномальных данных с использованием изоляционного леса



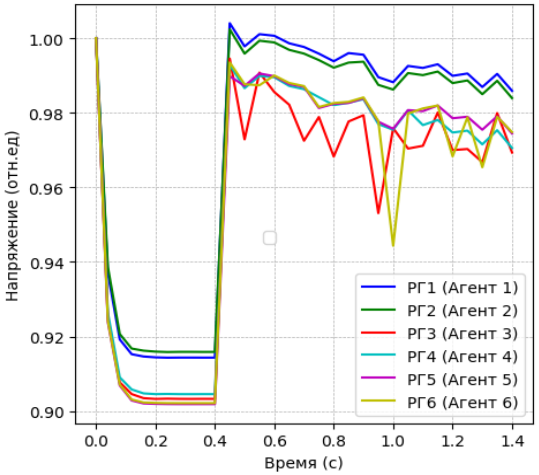
а) В отсутствие КА



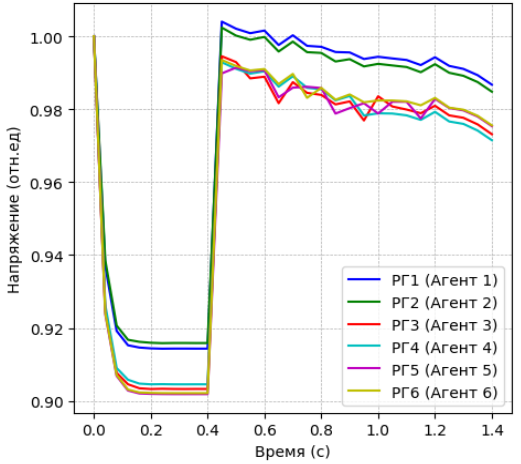
б) FDI-атака



в) Подавление последствий FDI-атаки



г) Hijacking-атака



д) Подавление последствий Hijacking-атаки

Рис. 5.5. Результаты достоверизации данных при кибератаках

Использование предлагаемого подхода позволит своевременно обнаруживать место локализации кибератак, не допускать распространение кибератак на соседние контроллеры и восстанавливать качество данных, используемых при вторичном регулировании напряжения.

Эффективность предложенного подхода подтверждена на примере моделирования кибератак на системы управления микросетями.

1. Важным и актуальным направлением является решение вопросов информационной безопасности (кибербезопасности) цифровых электроэнергетических объектов. Направление характеризуется быстро и динамично развивающейся нормативной базой в области информационной безопасности.
2. В существующей отраслевой практике, к сожалению, недостаточно нормативных документов, которые бы давали методические рекомендации по обеспечению кибербезопасности ЭЭС с конкретно применяемыми цифровыми устройствами, системами защиты, автоматики и управления.
3. Жесткие сроки по реализации планов перехода на доверенные программно-аппаратные комплексы и решений вопросов кибербезопасности, а также условия и переход противостояний из активной фазы боевых действий в киберсферу, стимулируют развитие новых исследований в области информационной безопасности (кибербезопасности) ЭЭС и разработку методов по ее обеспечению.
4. Предложенные методики будут полезны для применения в системах защиты, автоматики и управления и, прежде всего, где существует информационный обмен между цифровыми объектами.
5. Целесообразно апробировать предложенные методики на цифровых энергообъектах, в том числе с распределенными энергетическими ресурсами.

1. Разработка методических рекомендаций по обеспечению кибербезопасности и связанных с ними других методик, которые направлены на оценку надежности, поскольку кибербезопасность является компонентом надежности.
2. Разработка типовых доверенных программно-аппаратных комплексов и типовых решений на доверенных программно-аппаратных комплексах на цифровых энергообъектах, в том числе включающих распределенные энергетические ресурсы.
3. Необходима реализация отраслевых НИОКР, направленных на обеспечение информационной безопасности энергообъектов с последующей апробации методик по оценке киберзащищенности с учетом опыта эксплуатации.
4. Перспективным является исследование новых вероятностных моделей, которые будут положены в основу методик оценки уровней защищенности и устойчивости цифровых объектов и всей электроэнергетической системы в целом.

Благодарю за внимание !!!

E-mail: gurina@isem.irk.ru