УДК 004.77 Вестник УрФО № 2(52) / 2024, с. 46–55

**Кузьмина У. В., Бачурин И. В., Михайлова О. Е.** DOI: 10.14529/secur240205

# *ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ТЕХНОЛОГИЧЕСКИХ СЕТЕЙ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ*

*В статье рассмотрены основы построения технологических сетей промышленных предприятий и подходы к обеспечению их защиты. Рассмотрена обобщенная структурная схема АСУ ТП промышленного предприятия. В статье представлен анализ статистики кибератак за 2023 год. Полигоном исследования послужили промышленные предприятия региона. На основе экспериментальных исследований по широкому спектру показателей безопасности получена статистика мер по обеспечению безопасности промышленных предприятий региона. На основе полученной статистики были разработаны рекомендации по обеспечению мер информационной безопасности промышленных сетей предприятий.*

***Ключевые слова:*** *информационная безопасность, кибератака, технологические сети, АСУ ТП.Kotelnikov N. D., Afanasyeva M. V., Barankova I. I.*

**Kuzmina U. V., Bachurin I. V., Mikhaylova O. E.**

# *PROBLEMS OF PROTECTING TECHNOLOGICAL INDUSTRIAL ENTERPRISES NETWORKS*

*The article discusses the basics of constructing technological net-works of industrial enterprises and approaches to ensuring their protection. A generalized block diagram of the automated process control system of an industrial enterprise is considered. The article provides an analysis of cyber attack statistics for 2023. The testing ground for the study was the industrial enterprises of the region. Based on experimental studies on a wide range of security indicators, statistics on measures to ensure the security of industrial enterprises in the region were obtained. Based on the statistics obtained, recommendations were developed to ensure information security measures for industrial networks of enterprises.*

***Keywords:*** *information security, cyber-attack, technological networks, auto-mated process control system.*

**Введение.**

Особенности построения архитектуры технологических сетей промышленных предприятий кардинально отличают ее от корпоративных ин-формационных систем: начиная от специфических протоколов передачи данных (Modbus, DP, FDL, FMS), используемого оборудования (датчики, программируемые логические контроллеры, OPC сервера и др.) и программного обеспечения (SCADA, MES системы), заканчивая средой, в которой они функционируют (цеха, производственные помещения). Плюсом к вышеперечисленному в рамках Индустрии 4.0 активно распространяется промышленный интернет вещей (IIoT) и все большее количество устройств подключается к инфраструктуре промышленной сети предприятий.

АСУ ТП строится как децентрализованная система, выполняющая ин-формационные, управляющие и вспомогательные функции и состоит из трех уровней [1]:

Уровень 1 – «полевой» уровень; датчики, исполнительные механизмы, локальные микропроцессорные системы.

Уровень 2 – автоматическое управление; программируемые логические контроллеры (далее ПЛК), получающие данные с «полевого» уровня, передающие данные на верхний уровень для принятия решения по управлению объектом и (или) процессом и формирующие управляющие команды для исполнительных устройств, а также промышленная сеть передачи данных;

Уровень 3 – операторское управление; управление производством; операторские (диспетчерские), инженерные автоматизированные рабочие места, промышленные серверы (SCADA-серверы) с установленным общесистемным и прикладным программным обеспечением, телекоммуникационное оборудование (коммутаторы, маршрутизаторы, межсетевые экраны, иное оборудование), а также каналы связи; формирование, выдача производственно-технологической информации, обмен информацией между цехом и предприятием, прием информации о производственном задании.

Ввод и обмен данными между подсистемами АСУ ТП осуществляется автоматически в режиме реального времени, при этом оператор-технолог осуществляет контроль функционирования системы и участвует в управлении. Режим работы круглосуточный, непрерывный (за исключением запланированных ремонтных работ). В корпоративных информационных системах основной защищаемый ресурс – информация, а цель – обеспечение конфиденциальности. В технологических системах первостепенной задачей является сохранение непрерывности производства, которую обеспечивают доступность и целостности данных. АСУ ТП имеют жестко фиксированную конфигурацию, не допускающую существенных изменений (обновления ПО, использование наложенных средств защиты, корректировка настроек «по умолчанию»).

**Актуальность проблемы.**

На ряду с ростом устройств, подключаемых к сети, растет и количество хакерских атак на сети. По словам директора по развитию бизнеса в центре противодействия цифровым угрозам Solar JSOC Алексея Павлова: «На сегодня кибербезопасность - один из ключевых вопросов российских компаний». Атакам массово подвергаются крупные предприятия из топливно-энергетического сектора, финансовой отрасли, телеком-индустрии. Среди них - «Газпром», «Лукойл», «Норникель», «Сибур», Сбербанк и др.

В 2023 году в России и СНГ с наибольшим числом кибератак столкнулись организации в сферах промышленности (20% от общего количества инцидентов в регионе), финансов (17%) и ИТ (8%). Таковы данные ежегодного аналитического отчёта, основанного на статистике инцидентов, выявленных у пользователей Kaspersky Managed Detection and Response — решения по круглосуточному мониторингу, проактивному поиску и устранению киберугроз. Российские компании осознают необходимость защиты от целевых атак, поскольку их становится все больше, а последствия обходятся бизнесу очень дорого. Эта тенденция прослеживается не только на российском рынке: в опросе Cybersecurity Insiders 85% организаций-респондентов также не исключают возможности такой атаки на свою инфраструктуру в ближайшие 12 месяцев.

Статистика компании Positive Technologies так же подтверждает постоян-ный рост кибератак (рис. 1). Из них атаки на промышленность составляют 10% (рис 2.).

В связи с тем, что архитектура технологических сетей промышленных предприятий имеет очень сложную многоуровневую структуру, то и обеспече-ние ее защиты является сложной многоуровневой задачей. Для

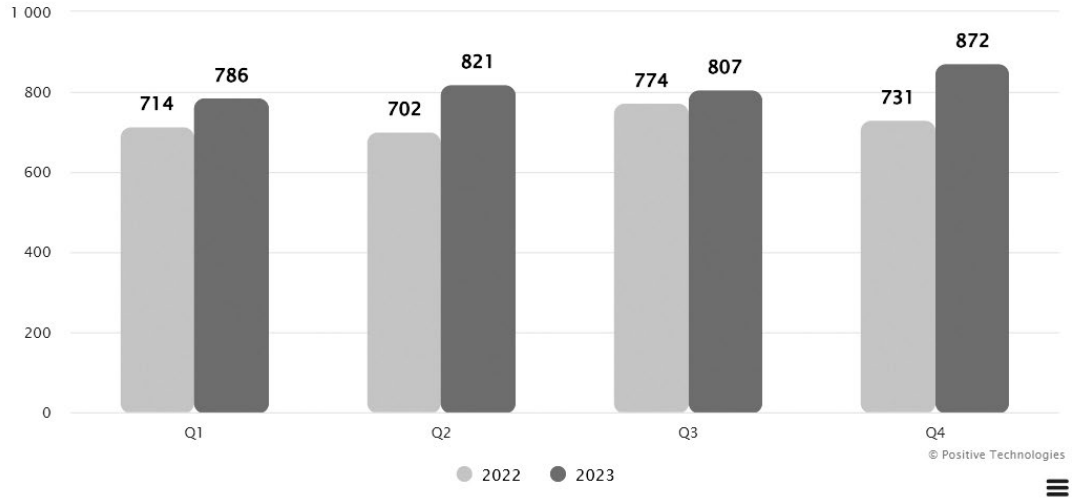


Рис. 1. Количество атак в 2022 и 2023 годах (по кварталам)

решения этой задачи необходимо учитывать требования законодательства для обеспечения защиты информации на критических информационных инфраструктурах [2-7].

**Постановка задачи.**

Объектом нашего исследования является автоматизированные системы управления технологическими процессами (АСУ ТП) промышленных предприятий региона [8-13].

Обобщенно сетевая инфраструктура АСУ ТП промышленных предпри-ятий имеет 3-уровневую иерархическую топологию сети передачи данных: яд-ро, уровень распределения, уровень доступа. Ядро сети отвечает за высокоскоростную передачу сетевого трафика. Каждое устройство уровня ядра обладает возможностью доступа к любому устройству пункта назначения сети. Устройства уровня ядра соединены между собой отдельными. На уровне распределения происходит суммирование маршрутов и агрегация трафика. В существующем решении уровни распределения и ядра совмещены в одном устройстве. Уровень доступа отвечает за формирование сетевого трафика, выполняет контроль точек входа в сеть и предоставляет службы пограничных устройств. Компоненты АСУ ТП находятся в общей сети предприятия и подключены к автоматизированной системе управления производством (АСУП) с применением меж-

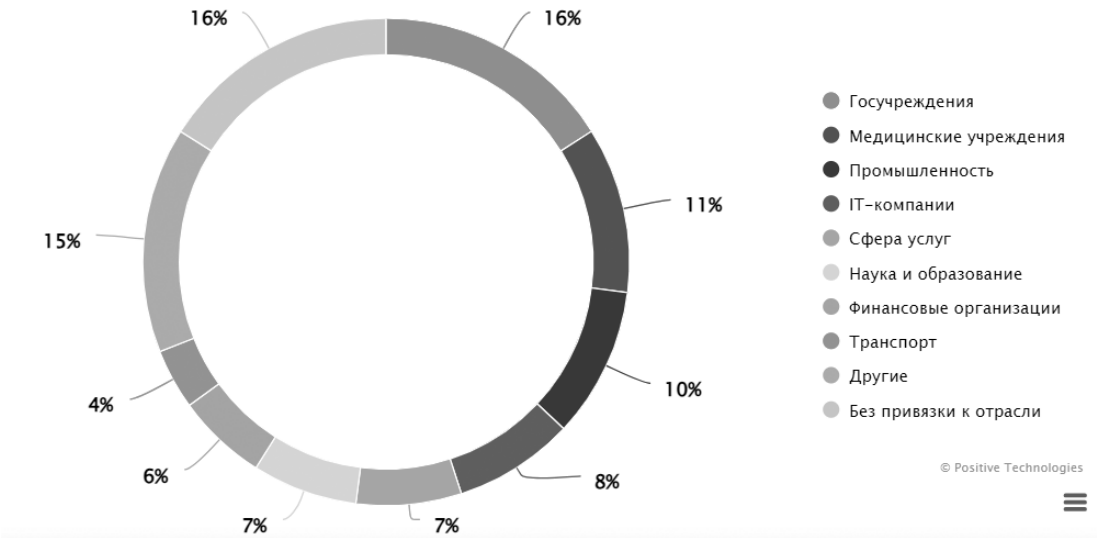


Рис. 2. Категории жертв среди организаций

сетевого экрана. Сеть АСУ ТП не имеет непосредственного соединения с сетью АСУП, для соответствующего взаимодействия два сервера имеют отдельные сетевые интерфейсы, подключенные в соответствующие сети.

**Методы оценки защиты технологических сетей промышленных предприятий.**

При обеспечении кибербезопасности технологической сети промышленного предприятия одинаково важны, как процессы разработки и реализации защитных мер, так и процессы проверок и контроля состояния защищенности [10]. Подобный контроль дает возможность провести проверку для установления валидности и актуальности используемых средств и систем защиты информации (СЗИ) [9]. На практике у большинства промышленных предприятий нет цельной, четко отлаженной СЗИ. Так, например, антивирусные программные средства установлены на многих АСУ ТП, чего не скажешь о системах обнаружения/предотвращения вторжений или правилах и регламентах реагирования на компьютерные инциденты. Вследствие чего возникает необходимость оценить положение дел и разобраться, какие меры по защите информации реализованы, а какие в обязательном порядке требуют немедленного внедрения. Аудит информационной безопасности (далее аудит ИБ) способствует получению наиболее точных данных о текущем состоянии предприятия в сфере обеспечения безопасности информации [9]. Своевременное обнаружение всех возможных актуальных уязвимостей и угроз безопасности, которые могут возникнуть из-за недостатка принятых мер защищенности, позволит обеспечить построение адекватной и эффективной СЗИ, которая будет соответствовать специфике предприятия.

Аудит ИБ занимает особое положение среди процессов контроля и про-верки, т.к. на данный момент для него не существует строгого нормативного определения. Согласно ГОСТ Р ИСО 19011–2021 [14] «аудит (audit): Система-тический, независимый и документированный процесс установления объектив-ного свидетельства и его объективного оценивания для получения степени соответствия критериям аудита» [4]. В области ИБ принято выделять четыре вида аудита такие как:

1. Экспертный направлен на выявление недостатков СЗИ с помощью экспертов по обеспечению безопасности информации (ОБИ);

2. Оценка соответствия требованиям российского и международного законодательства. Цель настоящего аудита – выявление недостатков СЗИ посредством анализа полноты исполнения требований по ОБИ регламентов, нормативно правовых актов и законодательства;

3. Инструментальный анализ. Данный вид предполагает выявление уяз-вимостей программного и программно-аппаратного обеспечения исследуемой системы;

4. Комплексный аудит включает в себя все вышеперечисленные виды проведения проверки [5].

Международный стандарт ISO 19011-2021 содержит общее представление о процессе аудита ИБ – термины, принципы, этапы и способ оценки компетентности аудитора. Руководствуясь данным документом, аудитор может грамотно и полно разработать программу аудита ИБ и все необходимые организационно-распорядительные документы (далее ОРД), список и содержание которых, от первого этапа «инициирования аудита» и до седьмого «завершение аудита», так же описаны в стандарте. Данные рекомендации применимы для аудита ИБ любых информационных систем, в том числе объектов КИИ. Конкретно для объектов КИИ ФСТЭК России разработал Приказы № 31 [5] и № 239 [2]. Данные документы необходимы для проведения выбранного вида аудита, т. к. содержат базовые наборы требований по «обеспечению защиты информации в автоматизированных системах управления производством и технологическим процессом» (АСУП и АСУ ТП). Кратко можно выделить основные вопросы проведения аудита, которые безусловно потребуют ответов [9]:

1. Какие силы обеспечения ИБ организованы на предприятии?

2. Какие ОРД по ОБИ (и в каком объеме/составе) разработаны и внедрены на предприятии?

3. Какие внедрены программные/ программно-аппаратные СЗИ и каков срок действия их сертификатов?

4. Какие осуществляются, как реализованы и чем регламентированы мероприятия для обеспечения безопасности информации?

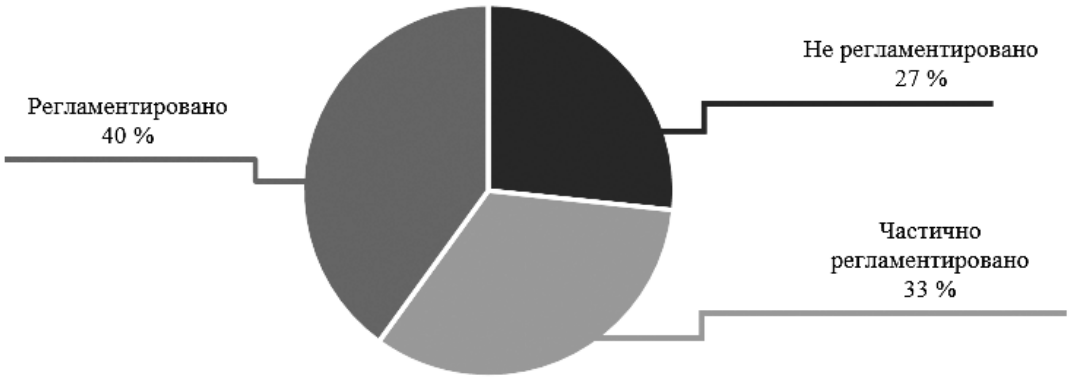


Рис. 3. Анализ полноты ОРД по ОБИ промышленных предприятий региона

**Результаты исследования защищенности технологических сетей промышленных предприятий.**

Выполнение требований 239-го приказа [2] необходимо для объектов критической информационной инфраструктуры (ОКИИ), признанных значимыми на основании проведенной процедуры категорирования, по правилам, утвержденным Постановлением Правительства РФ № 127 [6]. Незначимые объекты КИИ должны выполнять требования 31-го приказа [5], а также обязанности ч.2 ст. 9 Федерального закона № 187 [4] (требования данного ФЗ распространяются и на значимые объекты). Наименование мер защиты информации в обоих приказах идентичны, их различие состоит в том, что для незначимых объектов перечень мер определен для каждого из уровней значимости обрабатываемой в них информации, в то время как для значимых – по трем категориям значимости.

На основе проведенных исследований предприятий региона получена следующая статистика обеспечения безопасности промышленных предприятий региона (рис. 3, рис. 4).

В нормативных документах разработан базовый набор мер, которые в обязательном порядке должны выполняться для обеспечения защиты информации на предприятии. На диаграмме (рис. 4) представлен анализ полноты реализации базового состава технических мер КИИ, согласно нормативным документам. Обозначения мер на диаграмме (рис. 4) приведены согласно 239-му приказу [2].

Нулевой уровень показывает, что мера безопасности ничем не регламен-тирована и не реализована технически, первый уровень – разработаны и вне-дрены организационные меры защиты информации, второй – внедрены техни-ческие средства защиты информации, третий – разработаны и внедрены как организационные, так и технические меры защиты информации. Из диаграммы видно, например, что ИПО.0 (Регламентация правил и процедур информирования и обучения персонала), ИПО.1 (Информирование персонала об угрозах безопасности информации и о правилах безопасной работы), ИПО.2 (Обучение персонала правилам безопасной работы, ИПО.3 (Проведение практических занятий с персоналом по правилам безопасной работы), ИПО.4 (Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы) имеют нулевой уровень. Следовательно, по этим показателям либо полностью отсутствует, либо выполнены точечно требования безопасности. То же самое касается и показателей

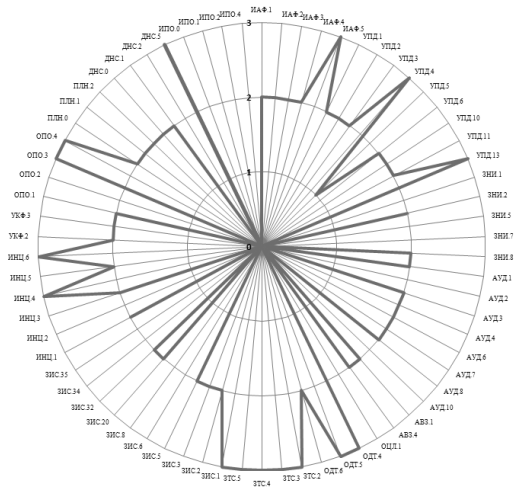


Рис. 4. Анализ полноты применения технических мер по ОБИ

ЗИС.35 (Управление сетевыми соединениями), ЗИС.36 (Создание (эмуляция) ложных компонентов автоматизированных систем), ЗИС.6 (Управление сетевыми потоками), ЗИС.8 (Сокрытие архитектуры и конфигурации автоматизированной системы) и т. д.

**Заключение.**

Проведенное исследование ИБ показало, что текущее со-стояние АСУ ТП в сфере обеспечения безопасности информации, не в полной мере удовлетворяет требованиям Приказов № 235, 239 ФСТЭК России. По результатам исследования ИБ составлены перечни организационных и технических мер, применение которых позволит перекрыть необходимый базовый набор мер обеспечения безопасности, регламентированный Приказами ФСТЭК России. Базовый набор мер защиты информации необходимо адаптировать в соответствии с применяемыми информационными технологиями и особенностями функционирования значимого объекта. Меры: контроль доступа из внешних систем, антивирусная защита электронной почты и иных сервисов, защита беспроводных соединений, управление перемещением виртуальных машин и обрабатываемых на них данных - следует исключить, т. к. они не применимы ввиду отсутствия технологий. В адаптивный набор необходимо включить меры группы «Предотвращение вторжений»: регламентация правил и процедур предотвращения вторжений, обнаружение и предотвращение компьютерных атак, обновление базы решающих правил. В результате исследования предложены общие рекомендации по реализации организационных и технических мер защиты информации на промышленных предприятиях.

Управление рисками ИБ АСУ ТП должно базироваться на требованиях ГОСТ Р ИСО/МЭК 27005. Управление рисками ИБ АСУ ТП должно включать:

а) инвентаризацию и классификацию активов АСУ ТП, включая инфор-мацию, обрабатываемую и хранящуюся в АСУ ТП;

б) оценку эффективности существующих мер и контроля по ИБ, включая выявление недостатков и уязвимостей обеспечения ИБ АСУ ТП, а также оценку рисков ИБ АСУ ТП;

в) планирование процессов и мер по ИБ АСУ ТП, направленных на снижение рисков, в том числе внесение изменений в существующие процессы и меры;

г) реализацию планируемых процессов и мер, осуществление контроля за выполнением планов и оценку достигнутых результатов.

Оценка рисков в отношении каждой из АСУ ТП должна осуществляться:

а) на плановой основе для АСУ ТП - не реже одного раза в три года;

б) постоянно с учетом изменений в технологических процессах, архитектуре и инфраструктуре (вычислительной, сетевой, КИПиА) АСУ ТП, а также по результатам мониторинга, аудитов ИБ АСУ ТП, инцидентов ИБ и оценки эффективности процессов и мер по обеспечению ИБ АСУ ТП.

Ответственность за проведение и координацию работ, связанных с управлением рисками нарушения ИБ АСУ ТП, включая утверждение результатов оценки рисков, утверждение планируемых мер по снижению рисков и выделение требуемых ресурсов на реализацию этих мер, возлагается на руководителя, отвечающего за обеспечение ИБ АСУ ТП.

Актуальность сведений об АСУ ТП должна поддерживаться путем проведения инвентаризации не реже одного раза в год. Ответственность за организацию регулярной инвентаризации должен нести руководитель, ответственный за обеспечение ИБ АСУ ТП.

В случае изменений в составе оборудования или ПО, сетевой или вычис-лительной инфраструктуры АСУ ТП эксплуатационный персонал АСУ ТП должен передать сведения об этих изменениях для актуализации информации в паспорте ИБ АСУ ТП.

Согласно Стандарту, сеть АСУ ТП должна быть разделена на «зоны». Нарушение связи между зонами АСУ ТП не должно приводить к остановке технологического процесса, он должен продолжаться, в режиме ограниченной функциональности, до восстановления связей между зонами.

Выделяют пять зон:

1) Зона систем управления содержит системы управления технологи-ческими процессами и представляет собой систему, с архитектурой человеко-машинного интерфейса – SCADA.

2) Зона систем промышленной безопасности включает системы противоаварийной защиты (далее - ПАЗ), обеспечивающих распознавание отклонения процесса от заданных параметров и оповещение об аварийных ситуациях, а также автоматическую остановку технологического процесса в случае обна-

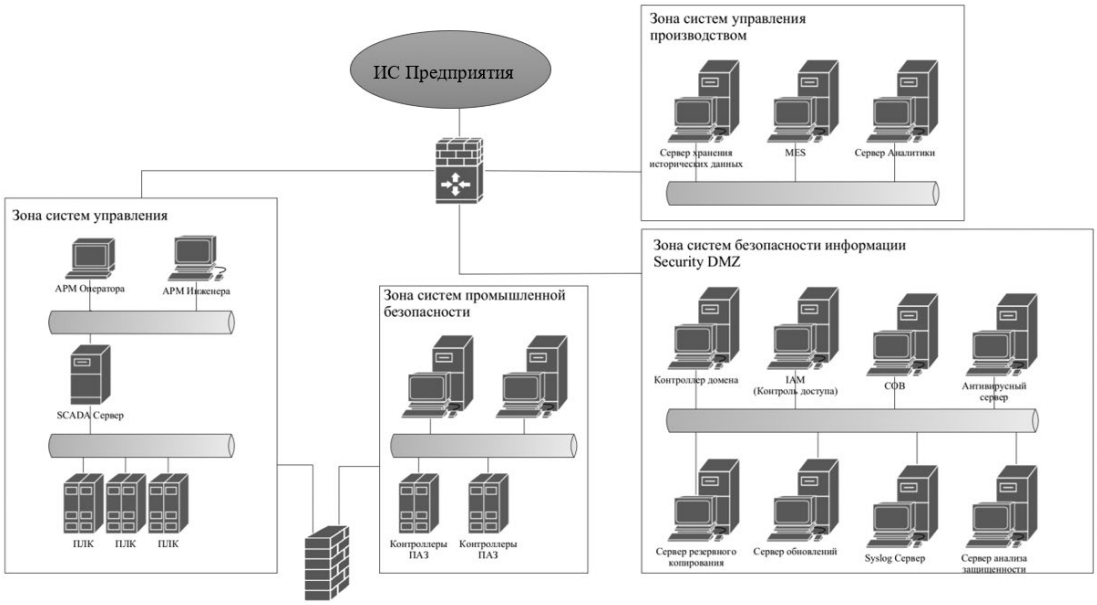


Рис. 5. Пример практической реализации концепции МЭК 62443 на обобщенной структурной схеме АСУ ТП промышленного предприятия

руженной критической неисправности. Данная зона должна быть максимально изолирована и защищена в соответствии с концепцией «защита в глубину».

3) Зона систем управления производством. К данной зоне, как прави-ло, относят системы, размещенные на уровне выше, чем SCADA, и не оказы-вающие прямое влияние на ход технологического процесса. Это могут быть системы класса Historian, системы оперативного управления производством. Например, MES, системы класса Intelligence и другие.

4) Зона управления СЗИ располагаются технические, программные и программно-аппаратные средства, обеспечивающие защиту 1-3 зон от угроз безопасности информации. Такими средствами могут быть: сервера - сбора и анализа данных, антивирусной защиты, резервного копирования; контроллер домена, системы обнаружения вторжений, и т.д.

5) Демилитаризованная зона (далее - ДМЗ) содержит технические или программные средства, которые обеспечивают взаимодействия между выше-описанными зонами АСУ ТП и корпоративной сетью предприятия (рис. 5).

Подсистема защиты периметра должна обеспечивать защиту информации от несанкционированного доступа, сегментирование технологической сети и контролировать межсетевое взаимодействие между сегментами технологической сети, технологическими ДМЗ и корпоративная информационная структура (КИС).

## Литература


1. Информационное сообщение ФСТЭК России, Об утверждении ме-тодического документа ФСТЭК России «Методика оценки показателя состоя-ния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации». [Электронный ре-сурс] Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii

2. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

3. Приказ ФСТЭК России от 18 февраля 2013 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» [Электронный ресурс] Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235

4. Федеральный закон от 19 июля 2017 г. № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/zakony/federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz

5. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных систе-мах 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» [Электронный ресурс] Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31

6. Постановление Правительства 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» » [Электронный ресурс] Режим доступа: https: //fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/287-postanovleniya/1614-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-8-fevralya-2018-g-n-127

7. КИИ: обзор нормативной базы ФСТЭК России [Электронный ресурс] Режим доступа: https://ics-cert.kaspersky.ru/publications/reports/2018/06/25/obzor-normativnoy-bazy-fstek-rossii/

8. Афанасьева С.В., Кузьмина У.В. / Основные проблемы при работе с центрами мониторинга информационной безопасности //\Вестник УрФО. Безопасность в информационной сфере. 2023. № 1 (47). С. 51-58.

9. Баранкова И.И., Семавина Е.А., Михайлова У.В. / Аудит информа-ционной безопасности промышленных предприятий, направленный на оценку соответствия требованиям российского и международного законодательства / Вестник УрФО. Безопасность в информационной сфере. 2022. № 3 (45). С. 76-82.

10. Михайлова У.В., Быкова Т.В. / Аудит информационной безопасности предприятия ООО "Машиностроительный завод РИВС" // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 77-й международной научно-технической конференции. 2019. С. 416-417.

11. Михайлова У.В., Афанасьева М.В. / Аудит информационной безо-пасности предприятия ООО "АНСЕР" // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 77-й международной научно-технической конференции. 2019. С. 417-418.

12. Баранкова И.И., Михайлова У.В., Афанасьева М.В., Афанасьев М.Ю. / Принципы построения модели надежности системы защиты информации АСУ ТП доменной печи // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 77-й международной научно-технической конференции. 2019. С. 424.

13. Barankova, I.I., Mikhailova, U.V., Kalugina, O.B. / Analysis of the Problems of Industrial Enterprises Information Security Audit // Lecture Notes in Electrical EngineeringЭта ссылка отключена., 2020, 641 LNEE, p. 976–985.

14. Национальный стандарт Российской Федерации. ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента» [Текст], Принят Приказом Федерального агентства по техническому регулированию и метрологии от 21 апреля 2021 г. – 2021. – 41 с

## References


15. Informatsionnoye soobshcheniye FSTEK Rossii, Ob utverzhdenii me-todicheskogo dokumenta FSTEK Rossii «Metodika otsenki pokazatelya sostoya-niya zashchity informatsii i obespecheniya bezopasnosti ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii». [Elektronnyy re-surs] Rezhim dostupa: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii

16. Prikaz FSTEK Rossii ot 25 dekabrya 2017 g. № 239 «Ob utverzhde-nii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kritiche-skoy informatsionnoy infrastruktury Rossiyskoy Federatsii» [Elektron-nyy resurs] Rezhim dostupa: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

17. Prikaz FSTEK Rossii ot 18 fevralya 2013 g. № 235 «Ob utverzhde-nii trebovaniy k sozdaniyu sistem bezopasnosti znachimykh ob"yektov kritiche-skoy informatsionnoy infrastruktury Rossiyskoy Federatsii i obespecheniyu ikh funktsionirovaniya» [Elektronnyy resurs] Rezhim dostupa: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235

18. Federal'nyy zakon ot 19 iyulya 2017 g. № 187 «O bezopasnosti kri-ticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» [Elek-tronnyy resurs] Rezhim dostupa: https://fstec.ru/dokumenty/vse-dokumenty/zakony/federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz

19. Prikaz FSTEK Rossii ot 14 marta 2014 g. № 31 «Ob utverzhdenii trebovaniy k obespecheniyu zashchity informatsii v avtomatizirovannykh siste-makh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kri-ticheski vazhnykh ob"yektakh, potentsial'no opasnykh ob"yektakh, a takzhe ob"yektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudey i dlya okruzhayushchey prirodnoy sredy» [Elektronnyy resurs] Rezhim dostupa: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31

20. Postanovleniye Pravitel'stva ot 8 fevralya 2018 g. № 127 «Ob utverzhdenii pravil kategorirovaniya ob"yektov kriticheskoy informatsionnoy infrastruktury rossiyskoy federatsii, a takzhe perechnya pokazateley kriteri-yev znachimosti ob"yektov kriticheskoy informatsionnoy infrastruktury ros-siyskoy federatsii i ikh znacheniy» » [Elektronnyy resurs] Rezhim dostupa: https: //fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/287-postanovleniya/1614-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-8-fevralya-2018-g-n-127

21. KII: obzor normativnoy bazy FSTEK Rossii [Elektronnyy re-surs] Rezhim dostupa: https://ics-cert.kaspersky.ru/publications/reports/2018/06/25/obzor-normativnoy-bazy-fstek-rossii/

22. Afanas'yeva S.V., Kuz'mina U.V. / Osnovnyye problemy pri rabote s tsentrami monitoringa informatsionnoy bezopasnosti //\Vestnik UrFO. Bez-opasnost' v informatsionnoy sfere. 2023. № 1 (47). S. 51-58.

23. Barankova I.I., Semavina Ye.A., Mikhaylova U.V. / Audit informa-tsionnoy bezopasnosti promyshlennykh predpriyatiy, napravlennyy na otsenku sootvetstviya trebovaniyam rossiyskogo i mezhdunarodnogo zakonodatel'stva / Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. 2022. № 3 (45). S. 76-82.

24. Mikhaylova U.V., Bykova T.V. / Audit informatsionnoy bezopasno-sti predpriyatiya OOO "Mashinostroitel'nyy zavod RIVS" // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. Tezisy dokladov 77-y mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. 2019. S. 416-417.

25. Mikhaylova U.V., Afanas'yeva M.V. / Audit informatsionnoy bez-opasnosti predpriyatiya OOO "ANSER" // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. Tezisy dokladov 77-y mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. 2019. S. 417-418.

26. Barankova I.I., Mikhaylova U.V., Afanas'yeva M.V., Afanas'yev M.YU. / Printsipy postroyeniya modeli nadezhnosti sistemy zashchity informa-tsii ASU TP domennoy pechi // Aktual'nyye problemy sovremennoy nauki, tekh-niki i obrazovaniya. Tezisy dokladov 77-y mezhdunarodnoy nauchno-tekhnicheskoy konferentsii. 2019. S. 424.

27. Barankova, I.I., Mikhailova, U.V., Kalugina, O.B. / Analysis of the Prob-lems of Industrial Enterprises Information Security Audit // Lecture Notes in Electri-cal EngineeringЭта ссылка отключена., 2020, 641 LNEE, p. 976–985.

28. Natsional'nyy standart Rossiyskoy Federatsii. GOST R ISO 19011-2021 «Otsenka sootvetstviya. Rukovodyashchiye ukazaniya po provedeniyu audita sistem menedzhmenta» [Tekst], Prinyat Prikazom Federal'nogo agentstva po tekhnicheskomu regulirovaniyu i metrologii ot 21 aprelya 2021 g. – 2021. – 41 s

**КУЗЬМИНА Ульяна Владимировна,** кандидат технических наук, до-цент кафедры «Информатики и информационной безопасности», ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: u.mihaylova@magtu.ru

**БАЧУРИН Иван Владимирович,** аспирант 2 курса кафедры «Вычислительных машин, систем и сетей», ФГБОУ ВО «Национальный исследовательский университет «МЭИ». 111250, г. Москва, Красноказарменная улица, дом 14, стр. 1. E-mail: biv@ipc2u.ru

**МИХАЙЛОВА Ольга Евгеньевна,** студент кафедры «Информатики и информационной безопасности», ФГБОУ ВО «Магнитогорский государствен-ный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: olgamihailova01@mail.com

**KUZMINA Ulyana Vladimirovna,** Candidate of Technical Sciences, Associate Professor of the student of the Department of Computer Science and Information Security, Federal State Budgetary Educational Institution of Higher Education, Magnitogorsk State Technical University named after G.I. Nosov. 455000, Magnitogorsk, Lenin Ave. 38. E-mail: u.mihaylova@magtu.ru

**BACHURIN Ivan Vladimirovich,** 2nd year graduate student of the Depart-ment of Computer Machines, Systems and Networks, Federal State Budgetary Educational Institution of Higher Education "National Research University "MPEI". 111250, Moscow, Krasnokazarmennaya street, house 14, building 1. E-mail: biv@ipc2u.ru

**MIKHAYLOVA Olga Evgenevna,** student of the Department of Computer Science and Information Security, Federal State Budgetary Educational Institution of Higher Education, Magnitogorsk State Technical University named after G.I. Nosov. 455000, Magnitogorsk, Lenin Ave. 38. E-mail: olgamihailova01@mail.com