УДК 004.046, 004.056 DOI: 10.26102/2310-6018/2020.28.1.026

Проблемы внедрения новых подходов к информационной безопасности в энергетической отрасли

С.Е. Голиков
Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет», Севастополь, Российская Федерация

Резюме: Качество жизни современного общества напрямую зависит от функционирования энергетического сектора. Не смотря на предпринимаемые меры по защите энергетической инфраструктуры, статистика инцидентов информационной безопасности свидетельствует о существенных недостатках применяемой архитектуры безопасности, носящих системный характер. Вероятность проникновения вредоносного программного обеспечения на вычислительные комплексы энергетических компаний за последние годы существенно возросла, что может оказать сильное влияние на доступность, целостность и конфиденциальность систем технологической сети энергетической отрасли. В статье проанализированы инциденты информационной безопасности (ИБ), показана уязвимость энергетических объектов не только к хорошо спланированным атакам, но и к обычному вредоносному программному обеспечению. Выявлены особенности использования принципов информационной безопасности в энергетике, описан ландшафт существующих угроз и уязвимостей, определены недостатки применяемой модели безопасности. Автором дана обобщенная характеристика модели «нулевого доверия», которую предлагается использовать на объектах энергоснабжения, приведен сравнительный анализ двух подходов к информационной безопасности. Применение разработанной «дорожной карты» внедрения новой концепции информационной безопасности, дополненная описанием путей минимизации операционных рисков, позволяет существенно повысить качество предоставляемых услуг для критичных бизнес-приложений, обеспечить надежную защиту от современных угроз информационной безопасности и утечек данных, улучшить гармонизацию с требованиями, предъявляемыми законодательством по безопасности.

Ключевые слова: информационная безопасность в энергетике, концепция нулевого доверия, угрозы информационной безопасности, инциденты информационной безопасности, модели информационной безопасности, управление уязвимостями, минимальные привилегии.

Для цитирования: Голиков С.Е. Проблемы внедрения новых подходов к информационной безопасности в энергетической отрасли. *Моделирование, оптимизация и информационные технологии.* 2020;8(1). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/02/Golikov_1_20_1.pdf DOI: 10.26102/2310-6018/2020.28.1.026

Problems of implementing new approaches to information security in the energy industry

S.E. Golikov
Federal State Autonomous Educational Institution of Higher Education "Sevastopol State University", Sevastopol, Russian Federation

Abstract: The quality of life of a modern society directly depends on the functioning of the energy sector. Despite the measures taken to protect the energy infrastructure, statistics of information security incidents indicate significant shortcomings in the applied security architecture that are of systematic

nature. The likelihood of malicious software penetrating the computer systems of energy companies has increased significantly in recent years, which could have a strong impact on the availability, integrity and confidentiality of technological network systems. In the article analyzed information security (IS) incidents, shown the vulnerability of power facilities not only to well-planned attacks, but also to ordinary malicious software. The features of using the principles of information security in the energy sector are identified, the landscape of existing threats and vulnerabilities is described, the shortcomings of the applied security model are identified. The author gives a generalized characteristic of the "zero trust" model, which is proposed to be used at power supply facilities, and provides a comparative analysis of two approaches to information security. The application of the developed roadmap for the implementation of a new information security concept, supplemented by a description of ways to minimize operational risks, can significantly improve the quality of services provided for critical business applications, provide reliable protection against modern information security threats and data leaks, and improve harmonization with the requirements of the legislation for safety.

Keywords: information security in the energy sector, the concept of Zero Trust, information security threats, information security incidents, information security models, vulnerability management, minimum privileges.

For citation: Golikov S.E. Problems of implementing new approaches to information security in the energy industry. *Modeling, Optimization and Information Technology*. 2020; . Available from: https://moit.vivt.ru/wp-content/uploads/2020/02/Golikov_1_20_1.pdf DOI: 10.26102/2310-6018/2020.28.1.026 (In Russ).

Введение

Предприятия энергетики являются объектами критически важной инфраструктуры, их стабильная работа прямым образом влияет на качество жизни любого человека. Не менее 90% функционала данных предприятий «завязаны» на информационные технологии [1]. Не смотря на то, что энергетическая инфраструктура проектируется с целью противостояния всем видам угроз, в том числе и угрозам информационной безопасности, в последнее время все больше внимания уделяется вопросам управления инцидентами информационной безопасности (ИБ), выработке методических руководств, позволяющих вовремя зафиксировать и не допустить развития атак на ИТ-инфраструктуру энергетических компаний.

Статистика инцидентов говорит о том, что энергетика является одной из наиболее подверженных угрозам отрасль. На Рисунке 1 приведена статистика инцидентов ИБ по отраслям промышленности [3].

Одной из самых серьезных проблем являются инциденты, связанные со специализированными вирусами типа Stuxnet, Flame, BlackEnergy, Petya, обнаруженных в промышленных компьютерных системах [2].

По данным ICS-CERT [4] в 2015 г. было зарегистрировано 295 инцидентов кибербезопасности на объектах критической инфраструктуры США, из них 46 – в энергетическом секторе.

Рисунок 1 - Количество инцидентов ИБ по отраслям промышленности

В конце 2015 года в Украине был осуществлен ряд успешных атак, в ходе которых предположительно были изменены конфигурации RTU (программно-аппаратных устройств среднего уровня АСУ ТП), уничтожены данные на автоматизированных рабочих местах диспетчеров, распределенным атакам типа «отказ в обслуживании» были подвергнуты call-центры энергосетевых компаний. В результате были отключены семь 110 кВ и двадцать три 35 кВ подстанций, в пяти регионах страны объекты энергоснабжения были отключены на 6 часов [5].

В апреле 2016 г. в корпоративной сети немецкой АЭС Gundremmingen было обнаружено вредоносное ПО, включая W32.Ramnit и Conficker [6].

5 марта 2019 на объекте электроэнергетики на западе США произошел инцидент информационной безопасности, вызвавший перебои в работе оборудования предприятия. В течение десяти часов межсетевые экраны (МЭ), расположенные на границе сетевого периметра предприятия, подвергались атакам со стороны неустановленных злоумышленников, использовавших уязвимость данной модели устройств. В результате атак устройства перезагружались, что вызывало их кратковременную недоступность (около 5 минут при каждой перезагрузке). Это приводило к кратковременной потере связи между центром управления и устройствами, расположенными на объектах предприятия [5].

В марте 2019 г. произошли масштабные отключения электричества в Венесуэле. Были отключены 20 из 23 штатов. Власти Венесуэлы заявили, что причиной блэкаута стала атака на ГЭС, снабжающей электроэнергией почти всю страну, со стороны США [8].

Подобные инциденты хорошо показывают уязвимость объектов энергетики не только перед хорошо спланированными атаками (энергосистема Украины или ядерная программа Ирана [9]), но и перед «случайными» заражениями «обычным» вредоносным ПО.

По данным «Лаборатории Касперского» в I-ом полугодии 2019 года нападениям подверглись 41,6% компьютеров АСУ в энергетике, в результате чего было заблокировано множество обычных (не предназначенных для АСУ ТП) вредоносных программ. Среди них особую опасность представляют майнеры (2,9%), черви (7,1%) и различные многофункциональные шпионские программы (3,7%), заражение которыми может оказать негативное влияние на доступность и целостность АСУ ТП и систем технологической сети.

Категорирование вредоносной активности позволило выявить, что главными источниками угроз для компьютеров в энергетической инфраструктуре являются интернет, съемные носители и электронная почта [9].

Принимая во внимание вышесказанное, вероятность проникновения вредоносного ПО на компьютеры энергетических компаний за последние годы существенно возросла, что может оказывать сильное влияние на доступность, целостность и конфиденциальность систем технологической сети.

Постановка задачи

Рост количества инцидентов ИБ и уязвимостей на объектах энергетики, а также их разнообразие показывает неудовлетворительное состояние дел в данном направлении, не смотря на все предпринимаемые попытки. Для обеспечения защиты в настоящее время применяется подход, при котором составляется модель возможных угроз, а затем разрабатываются меры по их нейтрализации. Целью работы является обоснование применения концепции «нулевого доверия» в качестве замены традиционной архитектуры сетевой безопасности.

Особенности применения принципов информационной безопасности в энергетике

Вопросы информационной безопасности на предприятиях энергетического сектора регулируются Федеральным законом от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». К сожалению, до настоящего времени не закончилось формирование нормативных правовых актов, отсутствуют методические рекомендации [10].

Основным защищаемым объектом в энергетике является не столько информация, сколько технологический процесс. Атаки на энергетические объекты влияют не столько на утечку информации, сколько на нарушение технологического процесса и работу всей энергосистемы. Следовательно, система защиты ИБ должна базироваться на принципах целостности и доступности технологического процесса и автоматизированных систем управления.

Особое внимание стоит уделить технологическим участкам генерации энергии и доставки конечным пользователям.

Существующий ландшафт угроз и уязвимостей

Основными проблемами в области информационной безопасности в энергетике являются:

- слабая разработанность политик и процедур ИБ для технологических систем;
- наличие уязвимостей сетевой архитектуры. Формирование архитектуры энергетических сетей происходит на протяжении десятков лет, что

приводит к несогласованности нормативной базы и регуляторной политики;

- уязвимости процессов авторизации, разграничения доступа и регистрации событий и инцидентов. Часто, в технологических сегментах вопросами ИБ занимаются подразделения, ответственные за эксплуатацию расположенных там программных систем, сотрудники которых не имеют специальных знаний и навыков;
- отсутствие средств защиты от вредоносных программ. Большое количество устаревшего аппаратного и программного обеспечения, обслуживающего технологические процессы, не позволяет установить современное антивирусное ПО, требовательного к вычислительным ресурсам;
- постепенная децентрализация архитектуры ввиду внедрения «зеленой» энергетики;
- наличие уязвимостей в области защиты физического и логического периметров.

Как правило, каналы связи между технологическими объектами, со смежными объектами, подрядчиками либо слабо, либо совсем не защищены. Множество объектов расположено в «плохо контролируемой зоне», в том числе жилых домах, общедоступных местах.

На Рисунке 2 приведены основные угрозы для объектов энергетической структуры и применяемые в настоящее время решения по снижения операционных рисков.

Рисунок 2 - Стандартная модель угроз

Исходя из вышесказанного, становится очевидным, что применение стандартного подхода к ИБ в условиях оперативных изменений технологических схем, морально устаревшей программно-аппаратной базы, не позволяет обеспечить надежную защиту.

Характеристики традиционного подхода к информационной безопасности

Традиционная архитектура информационной безопасности разделяет различные сети (или части одной сети) на зоны, разделенные одним или несколькими межсетевыми экранами. Каждой зоне предоставляется определенный уровень доверия, определяющий сетевые ресурсы, эксплуатация которых разрешена. Ресурсы, наиболее подверженные угрозам, например, веб-серверы, размещаются в так называемой «демилитаризованой» (DMZ) зоне, где трафик можно контролировать (Рисунок 3)

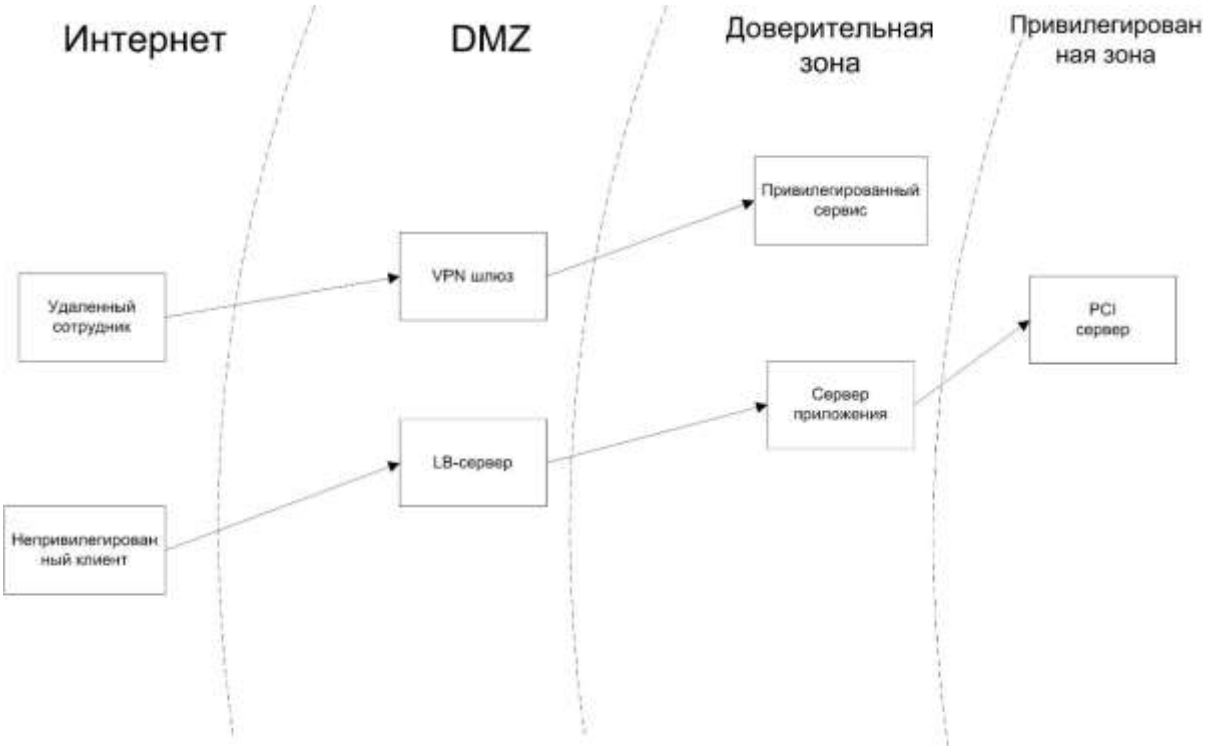

Рисунок 3. Традиционная модель ИБ

Недостатками данного подхода к организации информационной безопасности являются:

- отсутствие внутризоновой проверки перемещения;
- отсутствие гибкости в размещении хостов (как физического, так и логического);
- существование отдельных точек отказа;
- дискретность проверок.

Часто используемые в традиционной архитектуре виртуальные частные сети (VPN) позволяют пользователю проходить аутентификацию для получения IP-адреса в удаленной сети. После этого, трафик направляется с устройства в удаленную сеть, где он декапсулируется и маршрутизируется, что позволяет злоумышленнику при определенных условиях беспрепятственно попасть внутрь сети.

Для попадания во внутрь сети достаточно скомпроментировать хотя бы один хост в интересующей зоне. После этого, можно атаковать сеть изнутри. Скомпроментировав зону с низким уровнем безопасности, можно продвигаться к зонам с более высокой безопасностью.

Исходя из вышесказанного, становится очевидным, что существующая модель безопасности не обеспечивает надлежащую степень защиты. Обход периметра защиты для вредоносных программ не представляет сложности, т.к. МЭ при передачи между зонами анализируют только IP источника и получателя. Хотя применение защиты на периметре, позволяет обеспечить определенный уровень безопасности, ее роль, в качестве основного механизма защиты, требует пересмотра.

Концепция «нулевого доверия» (Zero Trust). Краткое описание

В 2010 г. компания Forrester предложила концепцию «нулевого доверия» или Zero Trust [11]. Данная концепция построена на нескольких фундаментальных утверждениях:

полное отсутствие доверия к кому-либо;

- внешние и внутренние угрозы существуют в сети постоянно;
- сетевое расположение недостаточно для установления доверительных отношений в сети;
- каждое устройство, пользователь и сетевой поток проходят проверку подлинности и авторизацию при каждом запросе доступа к какому-либо устройству внутри или за пределами сети;
- политики безопасности изменяются в динамике, принимая во внимание как можно больше источников данных;
- любая активность протоколируется.

Целью концепции является защита от современных угроз и утечек данных, при этом обеспечивая максимальную гармонизацию с законодательством по безопасности.

На Рисунке 4 показан пример архитектуры системы, построенной на принципах «нулевого доверия».

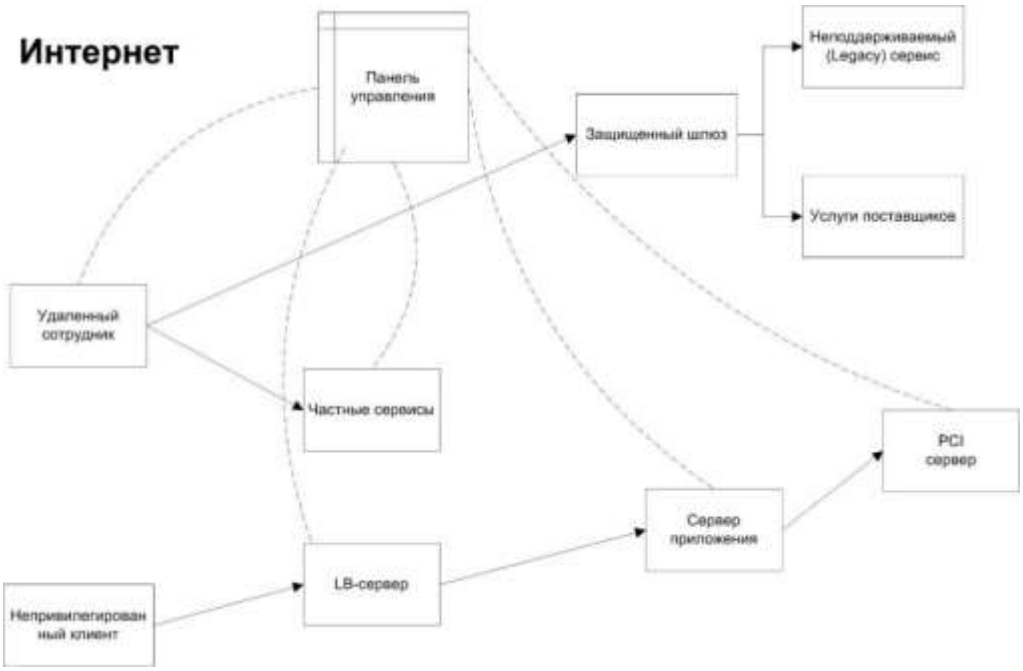

Рисунок 4 - Модель ИБ с использованием концепции «нулевого доверия»

Все запросы маршрутизируются «панелью управления», которая координирует и управляет всеми остальными компонентами, называемыми «панелями данных». Панель управления разрешает доступ к ресурсам только от прошедших авторизацию устройств и пользователей, и получивших соответствующие права доступа. После предоставления доступа панели данных принимают запросы только от тех пользователей и устройств, доступ которых санкционирован панелью управления.

Изначально концепция «нулевого доверия» включала три ключевых компонента:

- авторизация пользователя / приложения/ устройства;
- стратегия минимума привилегий, строгий контроль доступа только к тем ресурсам, которые необходимы для выполнения работы;
- непрерывный сетевой мониторинг и аналитика.

Позже были добавлены компоненты, задействовавшие более высокий уровень – данные, приложения, пользователи:

- Zero-trust пользователи: аутентификация пользователей, постоянный мониторинг и управление их доступом и привилегиями;
- Zero-trust приложения: контроль всего стека приложений, особенно соединений между контейнерами или гипервизорами в облаке;
- Zero-trust данные: защита и управление данными, классификация, шифрование как при хранении, так и при передаче [12, 13].

Преимущества внедрения концепции «нулевого доверия» в энергетике

С момента своего зарождения концепция «нулевого доверия» развивалась как децентрализованная модель. При построении систем безопасности существует тенденция сосредоточиться на более изощренных аспектах инженерной проблемы в ущерб более скучным, но все же важным частям. Каждая из существующих моделей безопасности преследует одну и ту же цель: выявить угрозы для системы, а также выработать мероприятия, системы и процессы, снижающие опасность этих угроз.

Модель «нулевого доверия» требует обеспечения безопасности только информации, используемой для аутентификации и авторизации действий пользователей. Дополнительные требования к конечным точкам, например, полное шифрование диска, могут быть применены при помощи использования дополнительной политики.

Привязка оценки доверия к метаданным устройств и приложений позволяет создавать гибкие политики.

Zero Trust содержит четкое разделение между плоскостью управления и плоскостью данных. Плоскость данных состоит из приложений, брандмауэров, прокси-серверов и маршрутизаторов, которые непосредственно обрабатывают весь трафик в сети. Данные узлы позволяют быстро определить маршрут прохождения трафика. Плоскость данных имеет доступ к компонентам всей системы, поэтому важно, чтобы службы на плоскости данных не могли быть использованы для получения привилегий в плоскости управления и, следовательно, для перемещения вглубь сети. Уровень доверия может изменяться с течением времени, требовать регулярных проверок между доверенными лицами, для того, чтобы гарантировать соблюдение прав по разделению доступа. При реализации данного принципа наиболее подходящим решением являются арендованные токены доступа или сертификаты с коротким сроком службы.

В Таблице 1 показано сравнение двух подходов: традиционного и «нулевого доверия».

Таблица 1 – Сравнительная характеристика двух подходов к ИБ

Традиционный	модель угроз	действие во времени	статичные политики
	строится на основе предположения об исчерпывающем знании обо всех угрозах и методах защиты	права доступа после авторизации не меняются	не зависят от контекста выполнения, не меняются в зависимости от изменения контекста
Zero Trust	модель доверия	действие на транзакцию	динамичные политики
	данные классифицированы, фиксация на ограничении доступа к ним	возможность авторизации пользователя, устройства, приложения зависит от оценки рисков транзакции	меняются в зависимости от контекста пользователя, устройства, приложения, учитывая предыдущие транзакции

Таким образом, внедрение концепции «нулевого доверия» позволит обеспечить:

- изоляцию ассоциированных пользователей к приложениям и данным;
- разделение ключевых бизнес-функций;
- организацию безопасного гостевого доступа;
- использование региональных ограничений и создание локализованных веб-сайтов;
- бесшовную и безопасную интеграцию проводных/беспроводных сетей, использование персональных устройств в рабочих целях (BYOD), доступ при помощи виртуальных рабочих столов (VDI);
- изоляцию/сегментацию устройств «интернета вещей» (IoT) в корпоративной среде;
- изоляцию трафика в ЦОДе;
- единый домен маршрутизации на всем протяжении соединения;
- изоляцию маршрутов;
- обеспечение надлежащего качества сервиса для критичных бизнес-приложений.

Алгоритм внедрения концепции «нулевого доверия»

«Дорожная карта» внедрения Zero Trust должна включать в себя следующие шаги:

- определение реперных точек для данных, процессов и сети, сегментация зон сети;
- проведение классификации ресурсов и процессов;
- определение сегментов, зон вокруг «чувствительных» данных и процессов, установление параметров доступа на основе пункта 1, автоматизация правил и политик базового доступа безопасности, аудит точек контроля доступа;
- мониторинг действий с использованием аналитики: оптимизация и интеграция существующих решений, построение логической архитектуры и определение мест, где будут применяться аналитические инструменты, выбор производителей оборудования и программного обеспечения;
- документирование всех регламентов, тестирование политик безопасности, проверка работоспособности системы.

При внедрении концепции Zero Trust в энергетической отрасли возможно возникновение следующих проблем:

1. Вследствие наличия специфичного ПО и протоколов передачи, в том числе, устаревших с несоответствующими духу времени механизмами безопасности, при внедрении концепции нулевого доверия необходимо проанализировать не только инфраструктуру энергетического объекта и технологических процессов, но и определить критические точки. Тогда задача безопасности будет заключаться в защите именно этих точек. Модель «нулевого доверия» работает со слоями. Как правило, внешний периметр связан с источниками данных и редко взаимодействует со всей системой. В качестве защиты критических точек можно ввести регистрацию протоколов запросов, наличие «клавиатурных шпионов», сетевого трафика.
2. Ввиду возможной некорректной работы существующих программных и программно-аппаратных комплексов с устанавливаемыми средствами защиты, необходимо провести оценку рисков и попытаться переконфигурировать существующие технические решения для повышения уровня ИБ, а также реализовать защиту при помощи организационных мер.
3. Вследствие того, что применение новой концепции может снизить скорость передачи данных по существующим каналам связи, перед внедрением новой концепции необходимо определить те сегменты сети, где следует обеспечить максимальную скорость данных и не использовать в них средства защиты информации, оказывающих существенное влияние на скорость загрузки каналов.
4. Так как оборудование, установленное на энергетических объектах, у которых отсутствует контролируемая зона, может стать точкой входа в технологические сети и привести к атакам на любые объекты, необходимо разработать дополнительные политики доверия устройств в данных сегментах, обеспечить жесткий контроль за доступом и контроль передаваемых данных.
5. Для упрощения процесса перехода к концепции Zero Trust в первую очередь необходимо развернуть систему контроля привилегированных пользователей (PAM), которая позволит проводить анализ и контроль учетных записей, а также доступа привилегированных пользователей и системных администраторов. Отсутствие модели выдачи минимальных привилегий обесценивает все преимущества модели «нулевого доверия».

Заключение

В работе рассмотрены особенности информационной защиты энергетических объектов, показаны недостатки системы информационной безопасности, применяемой в настоящее время. Дано обоснование применения концепции «нулевого доверия» в качестве замены традиционной архитектуры сетевой безопасности, приведено сравнение двух подходов, показаны преимущества концепции «нулевого доверия». Так как объекты энергетики имеют свою специфику, приведена обобщенная «дорожная карта» внедрения новой концепции, описаны пути минимизации потенциально возможных операционных рисков.

Для успешного внедрения концепции «нулевого доверия», необходимо провести оценку рисков не только опасных действий пользователей, но и самих ресурсов. Без внедрения новой стратегии, новых технологических решений безопасности для удаленного доступа, PAM, управления уязвимостями, «нулевое доверие» останется лишь теоретической концепцией.

ЛИТЕРАТУРА

1. Палей Л. Кибербезопасность в энергетике – задача государственного уровня. Доступно по адресу: http://lib.itsec.ru/articles2/focus/kiberbezopasnost-v-energetike-zadacha-gosudarstvennogo-urovnya (дата обращения 20.02.2020 г.).
2. Информационная безопасность энергетики России. *Реальность и перспективы. Материалы Smart Energy Summit 2018.* Доступно по адресу: http://smartenergysummit.ru/novosti/informaczionnaya-bezopasnost-energetiki-rossii.-realnost-i-perspektivyi (дата обращения 20.02.2020 г.).
3. Мелких А.А., Микова С.Ю., Оладько В.С. Исследование проблемы информационной безопасности АСКУЭ. *Universum: Технические науки*. 2016;6(27). Доступно по адресу: http://7universum.com/ru/tech/archive/item/3307 (дата обращения 20.02.2020 г.).
4. NCCIC/ICS-CERT Year in Review FY 2015, US Department of Homeland Security. Доступно по адресу: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf (дата обращения 20.02.2020 г.).
5. SANS-ICS, E-ISAC. TLP: White. Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. Доступно по адресу: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (дата обращения 20.02.2020 г.).
6. Detektion von Büro-Schadsoftware an mehreren Rechnern 25.04.2016. Доступно по адресу: http://www.kkw-gundremmingen.de/presse.php?id=571 (дата обращения 20.02.2020 г.).
7. В Венесуэле произошло масштабное отключение света. Доступно по адресу: https://ria.ru/20190325/1552099798.html (дата обращения 20.02.2020 г.).
8. Kaspersky ICS Sert. Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2019. Доступно по адресу: https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (дата обращения 20.02.2020 г.).
9. German nuclear plant infected with computer viruses, operator says. *REUTERS*. Доступно по адресу: http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS (дата обращения 20.02.2020 г.).
10. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ. Доступно по адресу:

http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 20.02.2020 г.).
11. Kindervag John, Balaouras Stephanie, Mak,Josh Blackborow Kelley. No More Chewy Centers: The Zero Trust Model Of Information Security. Доступно по адресу: https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682 (дата обращения 20.02.2020 г.).
12. Cunningham Chase. The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers. *FOR SECURITY & RISK PROFESSIONALS.* 2018(4). Доступно по адресу: https://www.em360tech.com/wp-content/uploads/2019/04/The-Forrester-Wave%E2%84%A2_-Zero-Trust-eXtended-ZTX-Ecosystem-Providers-Q4-2018-1-1.pdf (дата обращения 20.02.2020 г.).
13. Gilman Evan, Barth Doug. *Zero Trust Networks*. Sebastopol: O'Reilly Media, Inc., 2017.

REFERENCES

1. Palei L. Kiberbezopasnost v energetike – zadacha gosudarstvennogo urovnja. Dostupno po adresu:http://lib.itsec.ru/articles2/focus/kiberbezopasnost-v-energetike-zadacha-gosudarstvennogo-urovnya (data obrashcheniya 20.02.2020 g.).
2. Informatsionnaja bezopasnost energetiki Rossii. *Realnost I perspektivi. Materialy Smart Energy Summit 2018*. Dostupno po adresu: http://smartenergysummit.ru/novosti/informaczionnaya-bezopasnost-energetiki-rossii.-realnost-i-perspektivyi (data obrashcheniya 20.02.2020 g.).
3. Melkich A.A., Mikova S.Y., Oladko V.S. Issledovaniya problem informatsionnoy bezopasnosti ASKYE. *Universum: Technischeskie nauki*. 2016;6(27). Dostupno po adresu: http://7universum.com/ru/tech/archive/item/3307 (data obrashcheniya 20.02.2020 g.).
4. NCCIC/ICS-CERT Year in Review FY 2015, US Department of Homeland Security. Dostupno po adresu: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf (data obrashcheniya 20.02.2020 g.).
5. SANS-ICS, E-ISAC. TLP: White. Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. Dostupno po adresu: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (data obrashcheniya 20.02.2020 g.).
6. Detektion von Büro-Schadsoftware an mehreren Rechnern 25.04.2016. Dostupno po adresu: http://www.kkw-gundremmingen.de/presse.php?id=571 (data obrashcheniya 20.02.2020 g.).
7. V Venesuele proizoshlo masshtabnoye otklucheniye sveta. Dostupno po adresu: https://ria.ru/20190325/1552099798.html (data obrashcheniya 20.02.2020 g.).
8. Kaspersky ICS Sert. Landshaft ugroz dlya system promyshlennoi avtomatizazii. Pervoye polugodiye 2019. Dostupno po adresu: https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (data obrashcheniya 20.02.2020 g.).
9. German nuclear plant infected with computer viruses, operator says. *REUTERS*. Dostupno po adresu: http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS (data obrashcheniya 20.02.2020 g.).
10. Phederalniy zakon "O bezopasnosti kriticheskoi infrastrukturi Rossiiskoi Federazii" ot 26.07.2017 N 187-ФЗ. Dostupno po adresu: http://www.consultant.ru/document/cons_doc_LAW_220885/ (data obrashcheniya 20.02.2020 g.).

11. Kindervag John, Balaouras Stephanie, Mak,Josh Blackborow Kelley. No More Chewy Centers: The Zero Trust Model Of Information Security. Dostupno po adresu: https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682(data obrashcheniya 20.02.2020 g.).
12. Cunningham Chase. The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers. *FOR SECURITY & RISK PROFESSIONALS.* 2018(4). Dostupno po adresu: https://www.em360tech.com/wp-content/uploads/2019/04/The-Forrester-Wave%E2%84%A2_-Zero-Trust-eXtended-ZTX-Ecosystem-Providers-Q4-2018-1-1.pdf(data obrashcheniya 20.02.2020 g.).
13. Gilman Evan, Barth Doug. *Zero Trust Networks*. Sebastopol: O'Reilly Media, Inc., 2017.

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Голиков Сергей Евгеньевич, доцент, кафедра информационной безопасности, ФГАОУВО "Севастопольский Государственный университет", Севастополь, Российская Федерация.
e-mail: kcl@mail.ru

Sergei E. Golikov, Associate Professor, Information Security Department, Federal State Autonomous Educational Institution of Higher Education "Sevastopol State University", Sevastopol, Russian Federation.