**Форбс, 21.11.2024**

**<https://www.forbes.ru/tekhnologii/525533-fsb-predlozila-zasitit-ot-kiberatak-umnye-pribory-uceta-elektroenergii>**

**ФСБ предложила защитить от кибератак умные приборы учета электроэнергии**

Федеральная служба безопасности (ФСБ) и Минэнерго обсуждают ужесточение требований к защите информации в интеллектуальных системах учета электроэнергии, узнал Forbes. Предложения спецслужбы, если они будут утверждены, по данным источников, сделают обязательным оснащение умных счетчиков электроэнергии аппаратными средствами шифрования данных. По мнению компаний из энергетической отрасли, это приведет к увеличению стоимости приборов учета, по неофициальным оценкам, на 1000 рублей за каждый счетчик. IT-эксперт объясняет регулирование большим количеством кибератак на энергокомпании, зафиксированных за последние несколько лет, но собеседники в отрасли энергетики не припоминают таких инцидентов с «умными» приборами учета. Как рассказали Forbes в пресс-службе Минэнерго, с 2022 года сетевыми организациями (в отношении юридических лиц и ИЖС) и гарантирующими поставщиками (в многоквартирных домах) установлено более 6 млн интеллектуальных приборов учета (ИПУ). Наибольшее количество ИПУ установили группы компаний «Россети», «Интер РАО», «РусГидро». Внедрение дополнительного модуля криптографии в каждый счетчик приведет к удорожанию как самого прибора, так и всей системы интеллектуального учета в целом, рассказал Forbes заместитель генерального директора по технологическому развитию АО «Мосэнергосбыт» Геннадий Стрельцов: «Необходимо будет заменять все приборы учета, так как установку криптомодуля в счетчик можно сделать только на заводе-изготовителе».

Федеральная служба безопасности (ФСБ) и Минэнерго обсуждают ужесточение требований к защите информации в интеллектуальных системах учета электроэнергии, узнал Forbes. Предложения спецслужбы, если они будут утверждены, по данным источников, сделают обязательным оснащение умных счетчиков электроэнергии аппаратными средствами шифрования данных. По мнению компаний из энергетической отрасли, это приведет к увеличению стоимости приборов учета, по неофициальным оценкам, на 1000 рублей за каждый счетчик. IT-эксперт объясняет регулирование большим количеством кибератак на энергокомпании, зафиксированных за последние несколько лет, но собеседники в отрасли энергетики не припоминают таких инцидентов с «умными» приборами учета

Закодировать счетчики

ФСБ предложила Минэнерго ввести более жесткие требования к защите информации в интеллектуальных системах учета (ИСУ) электроэнергии, рассказали два источника Forbes в отрасли энергетики. По словам одного из них, ФСБ и Минэнерго обсуждают необходимость дополнительного шифрования в ИСУ. «Чтобы реализовать это требование, необходимо будет добавить на стороне конечного устройства определенное аппаратное решение с шифрованием», - говорит один из собеседников Forbes.

Российским энергетикам предписано создавать ИСУ электроэнергии двух типов. В двухуровневых ИСУ умные приборы учета подключаются непосредственно к информационно-вычислительным комплексам. В трехуровневой ИСУ между ними ставится устройство сбора и передачи данных (УСПД). Интеллектуальные приборы учета позволяют энергетикам дистанционно снимать показания счетчиков и отключать злостных неплательщиков.

Как рассказали Forbes в пресс-службе Минэнерго, с 2022 года сетевыми организациями (в отношении юридических лиц и ИЖС) и гарантирующими поставщиками (в многоквартирных домах) установлено более 6 млн интеллектуальных приборов учета (ИПУ). Наибольшее количество ИПУ установили группы компаний «Россети», «Интер РАО», «РусГидро». В министерстве также пояснили, что безопасность информации обеспечивается с помощью установки в УСПД сертифицированных ФСБ средств криптографической защиты информации (СКЗИ). «В трехуровневой ИСУ СКЗИ в интеллектуальных приборах учета не требуется с учетом принятия компенсирующих мер. По двухуровневой ИСУ работа по исследованию продолжается», - рассказали в Минэнерго. Там не уточнили, когда установка криптомодуля в прибор учета станет обязательной и будет ли это требование распространяться только на все новые счетчики или также и на уже введенные в эксплуатацию ИПУ.

Все нормативные акты по защите умных электросчетчиков сформированы, теперь производители решают вопрос, как обеспечить защищенность устройств, поясняет источник в одном из министерств. В то же время чиновники и силовики до сих пор ведут работу по согласованию протоколов связи умных счетчиков электроэнергии, добавил источник в одном из министерств. «Речь идет о создании единого стандарта для таких устройств и его обязательном применении в производстве», - говорит он.

По его словам, сейчас силовики и чиновники, отвечающие за защиту информации, видят риски использования функционала удаленного управления умных счетчиков для кибератак. «[Если хакеры] массово пошлют команды на отключение счетчиков, например в Москве, вся столица остается без электроснабжения. Последствия, вы же понимаете, какие, - размышляет источник в одном из министерств. - Одна из возможностей эти риски нивелировать - криптомодули [в счетчиках]». После того как силовики, чиновники и бизнес договорятся о стандартизации, то, по его словам, при благоприятном сценарии в течение 10 лет в России будет установлено 40 млн умных счетчиков электроэнергии.

Высокая дискуссия о нижнем уровне

Дискуссия о введении обязательного шифрования данных умных счетчиков электроэнергии ведется продолжительное время, говорят собеседники Forbes в отрасли энергетики. В июне 2021 года Минэнерго опубликовало базовую модель угроз безопасности информации ИСУ. Документ разработан Минэнерго совместно с ФСБ, Федеральной службой по техническому и экспортному контролю (ФСТЭК) и Минцифры.

Согласно этому документу, в приборах учета возможна реализация более сотни угроз безопасности информации. Его авторы тогда пришли к выводу, что угроза неправомерных действий в каналах связи и несанкционированного доступа к системе по беспроводным каналам может быть нейтрализована без применения СКЗИ. В то же время в июне 2021 года Николай Шульгинов (на тот момент министр энергетики) в своем письме руководителям сетевых организаций и гарантирующих поставщиков отметил, что базовая модель угроз безопасности информации подлежит пересмотру в срок до 31 декабря 2023 года в части использования в приборах учета электроэнергии СКЗИ, сертифицированных ФСБ России.

В 2023 году, по словам собеседника Forbes в отрасли, энергетики, чиновники и силовики работали над актуализацией документа. В апреле 2023 года в публикации журнала «Системы безопасности» сообщалось, что «ФСБ уже анонсировала необходимость установки СКЗИ в том числе на нижний измерительный уровень». Но в феврале 2024 года Минэнерго продлило действие документа до 31 декабря 2024 года. «На текущий момент 8-й Центр ФСБ продолжает заниматься актуализацией модели угроз, но пока окончательное решение не принято», - добавил собеседник Forbes.

Как пояснила исполнительный директор Ассоциации «Инсист Энерго» (объединяет восемь производителей приборов учета и УСПД) Наталья Готова, в соответствии с базовой моделью угроз, разработанной Минэнерго, и результатами проведенных испытаний защищенности трехуровневой системы ИСУЭ было принято решение, что в таких системах нет необходимости встраивать СКЗИ в сам прибор учета. «В отношении двухуровневой системы соответствующие испытания еще проводятся и не закончены. По итогам завершения будет дана оценка необходимости установки СКЗИ в ПУ, - рассказала Готова. - В настоящее время на рынке есть соответствующие технические решения СКЗИ и приборов учета с СКЗИ, в том числе и у членов ассоциации».

Дорогой прибор

В случае принятия решения о внедрении криптомодулей в умные счетчики их цена возрастет на 20% или 1000-2000 рублей в зависимости от модели за счет добавления нового элемента в устройство, полагает собеседник Forbes в отрасли энергетики. Другой источник в индустрии полагает, что СКЗИ на один прибор учета будет стоит около 1000 рублей, не считая наладки. Директор «Ассоциации участников рынка интернета вещей» Андрей Колесников также полагает, что стоимость криптомодуля не превысит 1000 рублей или 10% от средней цены «умного» электросчетчика.

Разница в цене счетчика с криптомодулем по сравнению с устройством без него будет зависеть от конкретных требований и характеристик криптомодуля, поясняет генеральный директор АНО «Умный многоквартирный дом» Никита Уткин. «Но в любом случае это не 5-10-процентное удорожание. Речь о том, что оно будет на десятки процентов и даже кратное. Вопрос, насколько это необходимо, востребовано и экономически эффективно, - рассуждает Уткин. - Пока позиция рабочей группы АНО, включающей профильных регуляторов, состоит в том, что, вероятно, столь затратные методы и инструменты могут не понадобиться за счет качественной отработки модели угроз и нарушителя и учета ее практических наработок на уровне систем». По его словам, АНО «Умный многоквартирный дом» не поддерживает как идею о принудительной замене существующих установленных приборов учета как с аналоговых на интеллектуальные, цифровые, так и идею о принудительной замене существующих установленных ИПУ на их аналоги с инструментами встроенной криптозащиты. «Разумное развитие этой тематики видится в области естественного замещения приборов учета с аналоговых на интеллектуальные по мере их выхода из периода допустимой эксплуатации и выхода из строя», - заключает Уткин.

Внедрение дополнительного модуля криптографии в каждый счетчик приведет к удорожанию как самого прибора, так и всей системы интеллектуального учета в целом, рассказал Forbes заместитель генерального директора по технологическому развитию АО «Мосэнергосбыт» Геннадий Стрельцов: «Необходимо будет заменять все приборы учета, так как установку криптомодуля в счетчик можно сделать только на заводе-изготовителе». Сотрудники «Мосэнергосбыта» в период с января 2022 года по октябрь 2024 года в многоквартирных домах установили более 1,11 млн ИПУ электрической энергии, в том числе в Москве - более 652 000 приборов и на территории Московской области - более 458 000 приборов.

При рассмотрении вопросов ИБ обычно рассматривают задачу не защиты всех устройств от незаконного воздействия, а снижения потерь от такого воздействия с учетом стоимости защиты, поясняет Стрельцов. «На сегодняшний момент в АО «Мосэнергосбыт» задача решается методами шифрования информации в канале «шлюз - программное обеспечение верхнего уровня», а также механизмами управления прибором учета. Злоумышленник может выключить небольшое количество приборов учета, этот факт будет сразу известен системе верхнего уровня, злоумышленник будет нейтрализован», - сказал он. Система защиты не позволит ему дать команду, например, на отключение всех счетчиков в доме, объясняет Стрельцов: «Смысла оборудовать каждый прибор учета нет, это приведет к существенному удорожанию системы без существенного снижения рисков».

Как сообщили Forbes в ПАО «Россети», с 1 января 2022 года, когда вступило в силу требование по внедрению только интеллектуальных счетчиков, компании группы установили более 1,9 млн интеллектуальных приборов учета. «Решение об использовании криптомодуля в приборах учета, безусловно, приведет к их удорожанию. Поэтому сейчас вместе с уполномоченными организациями идет поиск оптимального решения, которое позволит, с одной стороны, выполнить все требования по защите информации и исключит несанкционированное воздействие на прибор, с другой - минимизирует связанные с реализацией решения издержки», - сообщили в пресс-службе ПАО «Россети».

Интеллектуальные счетчики также устанавливала группа «Т Плюс» (основные собственники и 39,59% акций - структуры группы «Ренова» миллиардера Виктора Вексельберга ). Как указано в отчете об устойчивом развитии «Т Плюс» за 2022 год, в 2020-2022 годах установлено 214 000 умных приборов учета. К 2024 году их число превысило 500 000, рассказал собеседник Forbes, знакомый с ситуацией. В «Т Плюс» не ответили на запрос. Forbes также направил вопросы в компании «Русэнергосбыт», основанную группой ЕСН Григория Березкина, в «Интер РАО», «РусГидро», а также в ФСБ, ФСТЭК и Минцифры.

Новый рынок

За последние несколько лет в мире и, в частности, в России зафиксировано множество хакерских атак в энергетической отрасли, напоминает старший специалист по информационной безопасности компании «Криптонит» Евгений Дементов: «Внедрение криптомодуля в интеллектуальные приборы учета - это верный и неизбежный шаг в укреплении безопасности объектов критической информационной инфраструктуры». По его мнению, это позволит избежать умышленного искажения показаний приборов учета, обеспечить корректный расчет и прогнозирование потребления ресурсов энергосбытовым компаниям, минимизировать риски несанкционированного доступа к приборам учета.

Но два источника Forbes на рынке энергетики уверяют, что никогда не слышали, чтобы какой-то злоумышленник смог отключить потребителя, например квартиру, через умный прибор учета. В этом нет смысла, полагает один из собеседников Forbes. В то же время введение обязательного шифрования в приборе учета создает рынок для производителей средств киберзащиты, отмечают собеседники Forbes. Один из них упоминает компанию «ИнфоТеКС», у которой уже есть IT-решение для защиты счетчиков.

Компания «ИнфоТеКС» действительно имеет СКЗИ для приборов учета, сообщила руководитель продуктового направления «ИнфоТеКС» Марина Сорокина. По ее словам, это крипточип, он является частью решения для ИСУ, разработан в конце прошлого года и недавно получил сертификат ФСБ.

«Сейчас большое количество наших партнеров приобрели комплекты разработчика и начали встраивание крипточипов в свои изделия для поставки их своим заказчикам. Уже в первой половине следующего года на рынке будут появляться приборы учета и модули связи для приборов учета, оснащенные нашим крипточипом, - говорит Сорокина. - Если говорить про стоимость изделия, сейчас она составляет 1200-1600 рублей. Понятно, что при массовых закупках мы будем стремиться к нижней границе. И максимально стараемся удерживать стоимость даже сейчас, на этапе запуска производства, чтобы рынок сразу получал продукт по приемлемой цене».

По ее словам, сертифицированных решений СКЗИ для рынка приборов учета на данный момент не существует, хотя конкуренты «ИнфоТеКС» ведут активную работу в этой области. По данным ресурса Anti-Malware, решения для криптозащиты ИСУ также разрабатывают компании «С-Терра СиЭсПи» и АО НТЦ «Фискальная безопасность». Forbes направил запросы в эти компании.