РЕЗОЛЮЦИЯ

VI конференции «Информационная безопасность АСУ ТП КВО – 2018»

27–28 февраля 2018 г. в г. Москве состоялась VI конференция «Информационная безопасность АСУ ТП КВО». В ее работе приняли участие 337 человек. В течение двух дней было заслушано 32 доклада, проведен круглый стол по актуальным вопросам ИБ АСУ ТП. Ключевой темой обсуждения стало вступление в силу Закона № 187-ФЗ и принятие ряда подзаконных актов.

По итогам работы конференции сформулированы следующие предложения и рекомендации.

- Признать, что риски целенаправленных атак на АСУ ТП продолжают возрастать.
- Поддержать работу ФСТЭК России в части гармонизации № 187-ФЗ, Постановления Правительства РФ № 127-ПП, приказов № 235 и № 239 с приказами № 17, № 21, № 31 и иными законодательными актами ФСТЭК России.
- Отметить высокую оперативность ФСТЭК России в подготовке нормативных документов, необходимых для реализации положений № 187-ФЗ.
- Рекомендовать всем руководителям служб ИБ, ИТ и АСУ ТП промышленных предприятий в кратчайшие сроки изучить № 187-ФЗ, Постановление Правительства РФ № 127-ПП, приказы № 235 и № 239 и иные документы и незамедлительно инициировать на своих предприятиях работу по выполнению требований законодательства. Первоочередной задачей является формирование и согласование перечня объектов для категорирования.
- Обратить внимание на тот факт, что направление «Информационная безопасность» программы «Цифровая экономика Российской Федерации» крайне мало уделяет внимания практическим вопросам защиты информации в системах промышленной автоматизации.
- Рекомендовать заинтересованным лицам донести до первых лиц предприятий информацию об ответственности за нарушение правил эксплуатации объектов КИИ вплоть до заключения под стражу сроком на 10 лет.
- Обратить внимание на сложности начала финансирования работ по выполнению требований законодательства в связи с отсутствием в большинстве случаев соответствующих плановых расходов в бюджете предприятий. Тем не менее рекомендуется решать этот вопрос в приоритетном порядке.
- Обратить внимание, что обязанность реализовать требования подзаконных актов по защите КИИ распространяется не только на значимые объекты КИИ.
- Рекомендовать промышленным компаниям, которые не имеют критически важных объектов, учитывать рекомендации приказа № 31 ФСТЭК России при защите АСУ ТП.
- Производственным предприятиям учесть, что совсем не обязательно использовать сертифицированные средства защиты – можно организовать проверку соответствия в форме оценки защищенности и приемочных испытаний.
- Рекомендовать отдавать предпочтение российским продуктам АСУ ТП на новых объектах и при модернизации устаревших при условии качественного сопровождения их со стороны производителей.
- При проектировании новых АСУ ТП ЗОКИИ рекомендовать учитывать актуальные требования к безопасности и отдавать предпочтение тем производителям решений АСУ ТП, которые имеют встроенные механизмы защиты.
- Поддержать и одобрить деятельность зарубежных производителей промышленного оборудования и разработчиков АСУ ТП, направленную как на выполнение требований российского законодательство, так и на сотрудничество с отечественными разработчиками средств ИБ. Признать полезной практику Yokogawa подготовки документов для удовлетворения требований Закона № 187-ФЗ и рекомендовать другим производителям АСУ ТП подготовить аналогичные пакеты сопроводительной документации.
- Разработчикам АСУ ТП рекомендовать использовать при проектировании своих решений российские стандарты безопасной разработки программного обеспечения, подготовленные ФСТЭК России.
- Обратить внимание отечественных разработчиков на то, что новые продукты как в области АСУ ТП, так и средств безопасности для АСУ ТП должны не только удовлетворять требованиям импортонезависимости,

но и по своим базовым характеристикам не уступать зарубежным разработкам.
- Отметить рост информированности разработчиков АСУ ТП, особенно зарубежных, в области отечественной нормативно-правовой базы регулирования защиты информации АСУ ТП.
- Признать острый дефицит квалифицированного персонала имеющего компетенции как в части ИБ, так и АСУ ТП.
- Отметить, что сегментация сети покрывает большинство требований из проекта приказа № 239 ФСТЭК, кроме двух пунктов – обеспечение целостности и защита машинных носителей информации, для закрытия которых придется использовать другие решения.
- Признать крайне рискованной сложившуюся практику, при которой системные администраторы сами нарушают требования безопасности. В качестве эффективного инструмента борьбы с этим явлением рекомендуется использовать сертифицированные средства контроля привилегированного доступа.
- Рекомендовать промышленным компаниям изучить вопрос и начать подготовку к подключению в обозримой перспективе к системе ГосСОПКА.
- Владельцам значимых объектов КИИ рекомендовать сформировать собственный центр реагирования на компьютерные инциденты и подготовить его к интеграции с ГосСОПКА либо изучить возможность аутсорсинга услуг мониторинга инцидентов, операторы которых имеют возможность интегрироваться с ГосСОПКА. ■

В России в полтора раза увеличилось число компонентов АСУ ТП, доступных из Интернета

Количество доступных компонентов АСУ ТП в Глобальной сети растет с каждым годом: если в 2016 г. в России были обнаружены IP-адреса 591 подсистем, то в 2017-м уже 892. Такие результаты содержатся в исследовании компании Positive Technologies, где проанализированы угрозы, связанные с доступностью и уязвимостями АСУ ТП за минувший год. Наибольшее число компонентов АСУ ТП, присутствующих в Интернете, обнаружено в странах, где системы автоматизации развиты лучше всего, – США, Германия, Китай, Франция, Канада. За год доля США возросла почти на 10% и теперь составляет примерно 42% от общего числа (175 632). Россия поднялась на три позиции и занимает 28-е место. Эксперты Positive Technologies обращают внимание на увеличение доли сетевых устройств (с 5,06% до 12,86%), таких как конвертеры интерфейсов Lantronix и Moxa. Доступность подобных устройств, несмотря на их вспомогательную роль, представляет большую опасность для технологического процесса. Например, в ходе кибератаки на «Прикарпатьеоблэнерго» злоумышленники удаленно вывели из строя конвертеры фирмы Moxa, в результате была потеряна связь с полевыми устройствами на электроподстанциях. Среди программных продуктов в Глобальной сети чаще всего встречаются компоненты Niagara Framework. Подобные системы управляют кондиционированием, энергоснабжением, телекоммуникациями, сигнализацией, освещением, камерами видеонаблюдения и другими ключевыми инженерными элементами, содержат немало уязвимостей и уже подвергались взлому. Второе важное наблюдение исследователей касается растущего числа угроз в компонентах АСУ ТП. Число опубликованных уязвимостей за год выросло на 197, тогда как годом ранее стало известно о 115. Свыше половины новых недостатков безопасности имеют критическую и высокую степень риска. Кроме того, значительная доля уязвимостей в 2017 г. пришлась на промышленное сетевое оборудование (коммутаторы, конвертеры интерфейсов, шлюзы и т. д.), которое все чаще встречается в открытом доступе. При этом большинство обнаруженных за год недостатков безопасности в АСУ ТП могут эксплуатироваться удаленно без необходимости получения привилегированного доступа. По сравнению с 2016 г. лидеры поменялись. Первую позицию вместо компании Siemens теперь занимает Schneider Electric. В 2017 г. было опубликовано почти в десять раз больше уязвимостей (47), связанных с компонентами этого вендора, нежели годом ранее (5).

www.ptsecurity.ru