Вопросы защиты АСУ ТП критически важных объектов и пути их решения

В мире развернута гонка кибервооружений, в которую открыто включились не только наиболее развитые страны, но и международные преступные, в том числе террористические группировки. Иностранные спецслужбы и преступники предпринимают активные попытки использовать российскую информационную инфраструктуру для хищения информации, внедрения вредоносных программ в системы управления технологическими процессами критических важных объектов, создания плацдармов для проведения компьютерных атак на информационные системы Российской Федерации и третьих стран.

Большой интерес хакеров к взлому автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры, равно как и их высокую квалификацию подтверждают исследования различных профильных компаний и экспертных организаций. При этом значительная часть подключенных к Интернету АСУ ТП, использующихся на предприятиях энергетического комплекса, машиностроения и в других отраслях, уязвима даже для простейших хакерских атак. К сожалению, это можно сказать примерно о половине АСУ ТП российских предприятий.

Именно поэтому и Совет Безопасности, и руководство страны уделяют значительное внимание вопросам безопасности АСУ ТП критически важных объектов. В развитие принятых Советом Безопасности решений 15 января нынешнего года Президентом Российской Федерации был подписан указ о создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Данным указом определен федеральный орган, на который возложены полномочия по созданию такой системы, – Федеральная служба безопасности.

Угрозы АСУ ТП

При развитии информационно-коммуникационных технологий в Российской Федерации широко применяются зарубежные аппаратно-программные средства. Очевидна возможность наличия в таких средствах программных или программно-аппаратных закладок, а также недекларированных возможностей. Известны модели коммуникационного оборудования зарубежного производства, насчитывающие до сотни недокументированных команд, что позволяет дистанционно осуществлять неподконтрольное управление этим оборудованием. В большинстве зарубежных «защищенных микросхем» для коммерческого применения, в том числе предназначенных для защиты информации и продаваемых за пределы стран-изготовителей, предусмотрен «полицейский» режим, позволяющий получить доступ к ключевой информации и защищаемым данным, записанным в микросхемах. Кроме того, современные аппаратно-программные средства, в том числе используемые в информационных системах, прошедших проверку на соответствие действующим требованиям, содержат большое количество уязвимостей. При этом злоумышленники постоянно совершенствуют методы и средства выявления и эксплуатации существующих уязвимостей, чтобы преодолевать заслоны подсистем информационной безопасности.

Такое положение усугубляется тем, что в процессе эксплуатации защищенных информационных систем и автоматизированных систем управления регулярно происходят нарушения правил эксплуатации, обновляется и несанкционированно изменяется программное и аппаратное обеспечение, изменяются предписанные настройки средств защиты и программных компонентов. Сложившаяся практика осуществления иностранными фирмами технического обслуживания и удаленной настройки автоматизированных систем управления в целом или их составных частей, а также коммуникационного оборудования создают предпосылки для возникновения технологической и иной зависимости от иностранных государств.

На сегодняшний день применение зарубежной электронной компонентной базы является единственной возможностью создавать современную конкурентоспособную отечественную электронную аппаратуру, которая предназначается для решения сложных и актуальных функциональных задач в интересах государственных ведомств и организаций нашей страны. Чтобы нейтрализовать угрозы информационной безопасности, возникающие при использовании зарубежных аппаратно-программных средств, необходим комплекс скоординированных и спланированных правовых, организационно-технических и экономических мер. Эти меры должны быть направлены на создание и применение защищенных вычислительных средств, систем хранения данных, измерительной аппаратуры

и исполнительных устройств АСУ ТП, а также доверенного активного коммуникационного оборудования, предназначенного для построения сетей связи общего пользования и сетей специального назначения с высокой пропускной способностью. Необходимо создание защищенного системного программного обеспечения, включая защищенную операционную систему, мониторов виртуальных машин (гипервизоров) и сервисных утилит для обслуживания и диагностики элементов автоматизированных систем в защищенном исполнении, равно как и специализированного прикладного ПО для проектирования и разработки сложных технических систем (систем автоматизированного проектирования, пакетов расчетного и имитационного моделирования) с возможностью организации распределенных вычислений на суперЭВМ. Такое ПО должно обеспечивать достоверность данных на всех этапах жизненного цикла изделий за счет исключения недекларированных возможностей и использования эталонных моделей. Создание перечисленных средств должно сопровождаться их сертификацией по требованиям информационной безопасности.

Нормативная база

Базовым документом при обеспечении безопасности информационных систем критически важных объектов служат «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», утвержденные указом Президента Российской Федерации № 803 от 3 февраля 2012 г.

Одним из ключевых документов в части технических решений являются «Основные направления создания Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Это подтверждается указом Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

> Президент Российской Федерации дал поручение о принятии дополнительных мер по противодействию угрозам использования информационных технологий для несанкционированного вмешательства в работу АСУ ТП на критически важных и потенциально опасных объектах.

Сфера действия указа распространяется не только на правоотношения, связанные с обнаружением, предупреждением и ликвидацией последствий компьютерных атак, установлением причин компьютерных инцидентов в критической информационной инфраструктуре Российской Федерации и ее элементах, но и на все информационные ресурсы страны. Тем самым положения указа затрагивают интересы широчайших слоев российского общества. В качестве основных задач системы обнаружения, предупреждения и ликвидации последствий компьютерных атак рассматриваются не только прогнозирование ситуации в этой области, контроль степени защищенности критической информационной инфраструктуры и установление причин компьютерных инцидентов, но и обеспечение взаимодействия всех структур, которые занимаются защитой информации.

Постановка и решение задач защиты информации в АСУ ТП КВО требует активного и конструктивного сотрудничества российской общественности и профессионального сообщества. Кроме того, не следует забывать, что угрозы в информационной сфере носят трансграничный характер. Высокий уровень современных средств маскировки вредоносного программного обеспечения осложняет поиск местонахождения истинных источников угроз. Поэтому возникает объективная и неизбежная потребность в сотрудничестве с зарубежными партнерами. Необходимо объединение усилий самого широкого круга участников и, в перспективе, формирование системы международной информационной безопасности.

Помимо плановой законотворческой работы, которую ведут Правительство и Государственная Дума Российской Федерации, Президент Российской Федерации дал поручение о принятии дополнительных мер по противодействию угрозам использования информационных технологий для несанкционированного вмешательства в работу АСУ ТП на критически важных и потенциально опасных объектах.

На сегодняшний день федеральные органы государственной власти определили порядок использования сил и средств обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру Российской Федерации и разработали концепции использования сил и средств для ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре Российской Федерации.

Определены объемы и источники финансирования на реализацию программ и планов мероприятий в области обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры в целом, а также подготовлены предложения по корректировке утвержденных государственных программ и предложения в планируемые государственные программы.

Отраслевая специфика

Безусловно, надо учитывать, что в каждой отрасли существует своя специфика задач обеспечения безопасности. И эти задачи необходимо решать на уровне конкретной отрасли. Требования информационной безопасности обязаны выполнять предприятия всех отраслей, но в положениях федеральных законов, касающихся конкретных отраслей, эти требования должны быть определены более четко.

В сфере энергетики, например, необходимо согласовать законодательную и нормативную базы. Не полностью проработан в подзаконных актах Федеральный закон № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» – на сегодняшний день они касаются исключительно защиты объектов ТЭК и в недостаточной степени детализируют вопросы информационной безопасности. Кроме того, нормативные документы фактически отдают категорирование автоматизированных систем на откуп их владельцам, что неправильно. Владелец нередко просто не понимает, что его система критически важная, а иногда, к сожалению, не желает вкладывать средства в обеспечение необходимого уровня защищенности. Поэтому принятие решения о категорировании АСУ должно лежать на компетентном коллегиальном органе.

Все острее встает вопрос о необходимости создания единой политики в сфере организации взаимосвязей между сегментами энергетической инфраструктуры, представленной множеством компаний, и построения соответствующих корпоративного и технологического сегментов сети. Для этого требуются отраслевые стандарты.

За чей счет?

Масштабы предстоящей работы очень велики. Вопросы ее финансирования актуальны не меньше, чем вопросы нормативного обеспечения. В конечном счете все затраты закладываются в тарифы и конечную стоимость тех или иных товаров и услуг. Значит, необходима государственная целевая программа, включающая и вопросы категорирования объектов АСУ ТП, и вопросы финансирования их защиты. Тем более что эти объекты, как правило, объекты государственного значения, и немалая их доля относится к КВО. Некоторые эксперты считают, что необходимо централизованно осуществлять оценку стоимости каждого профиля защиты. Это не позволит компаниям, специализирующимся на обеспечении безопасности АСУ ТП, необоснованно завышать цены, даст ориентиры специалистам предприятий и позволит обосновывать стоимость мер защиты перед руководством. Возможно, государство тоже должно в какой-то степени участвовать в финансовом обеспечении внедрения средств защиты на критически важных и некоторых других объектах государственного значения. Но осуществляться это должно в сочетании с пристальным контролем за внедрением мер безопасности АСУ ТП, регулярными проверками соблюдения требований безопасности и самой серьезной ответственностью за их несоблюдение. Руководству компаний, осуществляющих деятельность в этой сфере, нужно осознать, что если государство на что-то тратит деньги, оно должно получать отдачу. В конечном счете речь идет об отсутствии угроз жизни и здоровью граждан России. ■

> Необходима государственная целевая программа, включающая и вопросы категорирования объектов АСУ ТП.

Редакция журнала благодарит представителей 8 Центра ФСБ России за предоставленные материалы и помощь в подготовке статьи

Полигон для будущих ИБ-специалистов

К новому учебному году Группа компаний МАСКОМ создала учебный класс для подготовки специалистов по защите информации в Амурском государственном университете. Учебно-лабораторный полигон (как его называют специалисты МАСКОМ) открылся 19 сентября.

В новых специализированных классах и лабораториях будущие специалисты сферы безопасности информационных систем смогут на практике отрабатывать навыки по противодействию несанкционированному доступу к компьютерным сетям и выявлению различных каналов утечки информации. К услугам учащихся системы, выпускаемые ГК МАСКОМ:

- автоматизированная система оценки защищенности технических средств от утечки информации по каналу ПЭМИН «Сигурд»;
- автоматизированная система оценки защищенности выделенных помещений по виброакустическому каналу «Шепот»;
- автоматизированная система измерения действующих высот случайных антенн и коэффициентов реального затухания электромагнитных сигналов «Стентор-мини»;
- автоматизированная система исследования эффекта акустоэлектрических преобразований в технических средствах и отходящих от них линиях «Талис»;
- автоматизированная система исследования эффекта акустоэлектрических преобразований в технических средствах и отходящих от них линиях в речевом диапазоне частот «Талис-НЧ-М1»;
- система постановки акустических и вибрационных помех «Шорох-3».

Подобные лаборатории на базе оборудования ГК МАСКОМ открыты в ряде ведущих вузов страны.

www.mascom.ru