

ОСТОРОЖНОСТЬ ИЗЛИШНЕЙ НЕ БЫВАЕТ

Проблемы кибербезопасности в ядерной отрасли

Число используемых компьютеров с каждым годом растет, а это создает все больше возможностей для кибератак.

(Фото: istockphoto.com)



Число компьютеров, которыми пользуются и с которыми взаимодействуют люди, с каждым годом растет, а это создает все больше возможностей для кибератак. Например, в современных автомобилях имеется не менее 12 цифровых каналов ввода/вывода: для управления двигателем, трансмиссией, радиоприемником, антиблокировочной системой тормозов, бесключевым доступом, противоугонными и телематическими устройствами и т.д. Потенциально всем этим устройствам присущи уязвимые места, подверженные взлому.

Компьютерные и информационные технологии развиваются очень быстро, порой опережая наше осознание возможных источников киберуязвимости и, в конечном итоге, возможной атаки. Кроме того, кибератаки не ограничиваются рабочим местом – их объектом может быть также частная жизнь людей.

Одна из главных целей МАГАТЭ в деле повышения кибербезопасности – укрепить культуру физической ядерной безопасности, изменить образ мысли людей и изменить то, как они оценивают не только внедрение технологии, но и ее использование.

“Если специалисты в ядерной сфере и члены их семей будут лучше осознавать не только свое физическое пространство, но и свое цифровое пространство, они будут проявлять большую осмотрительность в отношении онлайн-обмена информацией и

использования технологий. Информация, которая кажется безобидной, может быть объединена с другой информацией из других источников в интернете и может оказаться весьма опасной. Google и подобные интернет-поисковики часто являются первыми инструментами, которые хакеры используют при разработке плана атаки”, – говорит Дьюденхейффер.

Национальный координатор по вопросам безопасности и противодействия терроризму в Министерстве безопасности и юстиции Нидерландов Бен Говерс говорит, что в атомную отрасль постепенно проникает осознание этой угрозы. “Атомная промышленность сталкивается с двойной задачей расширения и углубления своих существующих средств защиты компьютерных и информационных сетей от киберугроз. Эта отрасль находится в – более или менее – начальной стадии разработки, внедрения и расширения надежных мер защиты систем информации и управления на ядерных установках”.

“Ведущую роль в этом динамичном процессе может играть МАГАТЭ”, – говорит Говерс.

Сообщество помощников

В октябре 2012 года был обнаружен компьютерный вирус «Красный октябрь». По оценкам он на

протяжении почти пяти лет собрал конфиденциальную информацию более чем в 60 странах, оставаясь при этом незамеченным. Информация, полученная из зараженных сетей, могла повторно использоваться для будущих кибератак. Такой уровень сложности в киберпреступности становится все более и более распространенным, и он представляет собой еще одну проблему, с которой должны бороться сотрудники служб физической ядерной безопасности.

МАГАТЭ оказывает поддержку государствам на всех уровнях в их усилиях по созданию надежных и испытанных программ информационной и компьютерной безопасности. МАГАТЭ организует региональные учебные программы, создает курсы для специалистов по физической ядерной безопасности, публикует руководящие принципы по кибербезопасности для ядерных установок и проводит регулярные международные встречи, на которых специалисты могут поделиться своим опытом и получить ответы других участников и экспертов МАГАТЭ на свои наиболее насущные вопросы.

В рамках организуемых МАГАТЭ миссий Международной консультативной службы по физической защите (ИППАС) МАГАТЭ проводит также оценку информационной безопасности.

ИППАС – служба всеобъемлющего обзора, доступная для всех стран, имеющих ядерный материал и установки, – консультирует государства по вопросам более эффективных способов защиты своих ядерных и радиационно опасных материалов.

Вопросами противодействия растущим киберугрозам занимаются многие организации. Большое значение в этой сфере имеют партнерские отношения. МАГАТЭ совместно с Международной организацией уголовной полиции (ИНТЕРПОЛ) и Европейским агентством сетевой и информационной безопасности (ЭНИСА) проводит международные учения, разрабатывает руководящие документы по кибербезопасности и организует учебные мероприятия.

@TOMIC 2012 – международные учения по кибербезопасности и событиям, связанным с физической ядерной безопасностью, в том числе по ядерной криминалистике, – являются одним из примеров участия МАГАТЭ в международной деятельности по повышению осведомленности в области кибербезопасности в целях защиты активов ядерных и других радиоактивных материалов. В этих учениях, проходивших при поддержке со стороны Нидерландов, участвовали 150 специалистов из 40 стран. Следующие учения – @TOMIC 2014 – пройдут в 2014 году.

Организатор учений @TOMIC Говерс говорит: “Поскольку МАГАТЭ пользуется авторитетом в ядерном мире, оно может играть стимулирующую и ведущую роль в реализации руководящих принципов и протоколов, а также в расширении осведомленности о мерах кибербезопасности”.

МАГАТЭ разработало ряд программ, цель которых – передача государствам знаний по этим вопросам, оказание им помощи в решении этой проблемы и в организации ответных действий.

Те же старые угрозы

Как указывает Дьюденхейффер, важно, чтобы государства-члены улавливали сходство между нынешними угрозами и теми, с которыми они сталкивались 50 лет назад.



Киберугрозы – это международная проблема. МАГАТЭ поддерживает государства-члены в их усилиях по разработке и испытанию мер компьютерной безопасности в целях защиты ядерных установок.

(Фото: istockphoto.com)

“Субъекты угрозы остаются прежними. Всегда есть криминальные элементы, которые пытаются что-то у вас похитить или шантажировать вас. Всегда есть те, кто выступает против вас и вашей работы, будь то террористы или недовольные сотрудники. Ядерные и радиологические установки всегда нуждаются в защите от таких угроз. Большая разница в том, что теперь, чтобы сделать свою грязную работу, эти субъекты угрозы могут использовать – на месте или удаленно – компьютерные системы”, – говорит этот эксперт по физической ядерной безопасности.

Саша Энрикес, Отдел общественной информации МАГАТЭ.