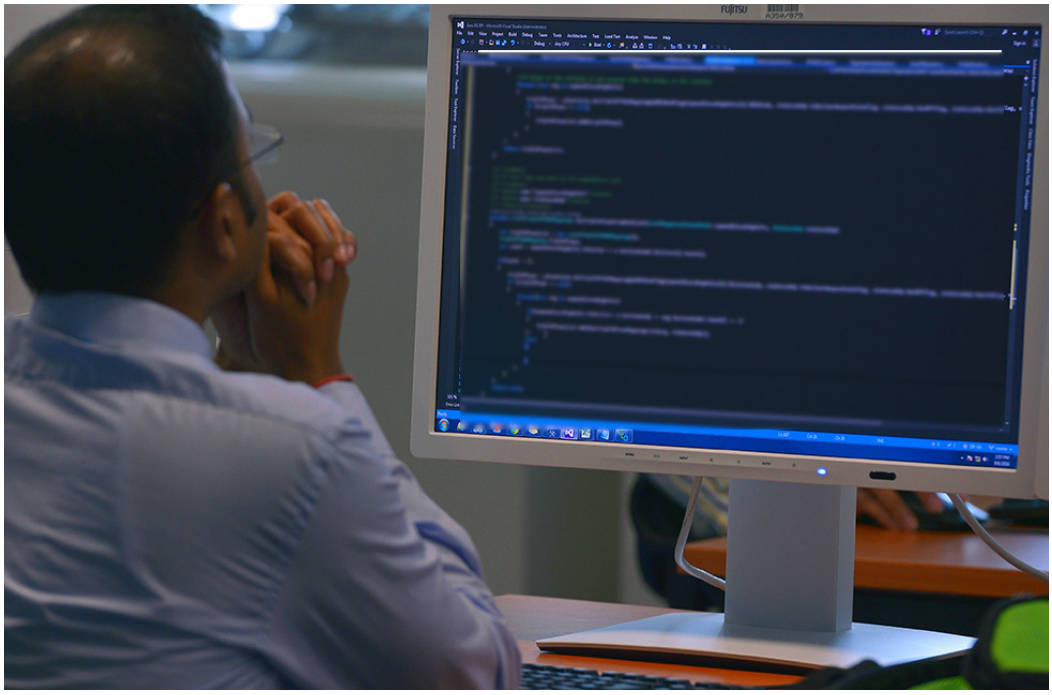
Оружие, охрана, ограждение и злоумышленники: Румыния усиливает компьютерную безопасность на ядерных установках

Лаура Хиль



(Фото: Д. Кальма/МАГАТЭ)

Посредством кибератаки с вашего компьютера можно удалить всю информацию и даже привести его в нерабочее состояние. Ничего хорошего в этом нет. А кибератака на АЭС может закончиться саботажем или хищением ядерного материала. Одним из важнейших компонентов физической ядерной безопасности является компьютерная безопасность, которая обеспечивает защиту цифровых данных, а также систем и сетей от злоумышленных действий.

“Развитие компьютерной техники и ее использование во всех аспектах ядерной деятельности изменили парадигму безопасности, – говорит Доналд Дьюденхейффер, сотрудник по вопросам безопасности информационных технологий МАГАТЭ. Информационная и компьютерная безопасность должны рассматриваться в качестве компонентов общего плана ядерной безопасности”.

В обеспечении физической ядерной безопасности давно доминирует идея физической защиты, которая часто обозначается формулой “оружие-охрана-ограждение”, однако преступники сегодня также используют компьютеры и как средство, и как цель своих нападений. Кибератака может привести к утрате информации по физической ядерной безопасности, саботажу в отношении ядерных установок, а в сочетании с физическим нападением – и к хищению ядерного или иного радиоактивного материала. Компьютеры в настоящее время играют важную роль в обеспечении ядерной безопасности, физической безопасности ядерных установок и управлении ими, поэтому насущно необходимо, чтобы все системы были надежно защищены от злоумышленных покушений.

“Мы все должны быть готовы к тому, чтобы защитить себя от агрессивной среды Интернета в эпоху цифровых технологий, – отмечает Дьюденхейффер. – Мы все используем компьютеры и должны четче осознавать, какие существуют угрозы, риски и способы защиты”. Регулирующие органы и операторы ядерных установок все отчетливее понимают важность компьютерной безопасности и стремятся укрепить свои программы физической ядерной безопасности. Румыния, по словам Дьюденхейффера, является одним из показательных примеров.

“Мы понимаем важность защиты от всех видов угроз, которые могут влиять на безопасное, надежное и бесперебойное функционирование наших ядерных установок, в том числе угроз в отношении компьютерной и информационной безопасности”, – говорит Мадалина Тронеа, координатор группы по ядерным постановлениям и стандартам Национальной комиссии по контролю за ядерной деятельностью (НККЯД) в Бухаресте, Румыния.

В 2012 году группа специалистов МАГАТЭ осуществила миссию Международной консультативной службы по физической защите в Румынию. Они представили властям список рекомендаций по дальнейшей разработке

надлежащей нормативно-правовой базы для защиты ядерных установок от различных угроз, в том числе кибератак.

Вскоре после этого группа сотрудников ядерных регулирующих органов из НККЯД начала работать над постановлением, которое вступило в силу в ноябре 2014 года. Это постановление посвящено защите систем, оборудования и компонентов, включая программное обеспечение для системы контроля и управления, которые имеют важное значение для ядерной безопасности, физической безопасности, гарантий и аварийного реагирования. В дополнение к этому постановлению НККЯД издала документ с изложением киберугроз с учетом новых угроз и последних событий в области компьютерной безопасности в отрасли по всему миру.

(Фото: НККЯД)

“Мы обращаем внимание на глобальный контекст и изменения как в отношении угроз, так и контрмер, – говорит г-жа Тронеа. – И мы делаем все возможное, чтобы обеспечить надлежащую профилактику и защиту от нарушений компьютерной безопасности, а также эффективное реагирование на такие случаи, если они произойдут”.

В том же году правительство Румынии утвердило Национальную стратегию ядерной и физической безопасности, которая включает цели непрерывного усиления компьютерной безопасности в ядерной отрасли.

Люди: проблема и решение

Исследования показывают, что большинство случаев нарушения компьютерной безопасности обусловлены человеческим фактором.

“Люди: развитие человеческого потенциала является одним из лучших инвестиционных направлений, – заявил г-н Дьюденхейффер. – Нам не нужен мир, состоящий из одних специалистов в области компьютерной безопасности. Нам нужен мир, в котором живут люди, осведомленные о рисках в области компьютерной безопасности и основных мерах защиты. Нам нужны грамотные работники и руководители”.

Благодаря учебным курсам МАГАТЭ, в которых Румыния принимает участие с 2013 года, в стране сложилась устойчивая сеть заинтересованных сторон. Через эту сеть заинтересованные стороны теперь обмениваются опытом в области физической ядерной безопасности и вместе работают над созданием мощных программ обеспечения информационной и компьютерной безопасности.

Посредством национальных учебных курсов, онлайнового обучения, совещаний экспертов и программ подготовки инструкторов МАГАТЭ работает с национальным руководством и заинтересованными сторонами в ядерной отрасли, чтобы лучше понять опасность киберугроз и обобщить передовую практику, позволяющую повысить уровень компьютерной безопасности. По мнению Дьюденхейффера, национальные учебные курсы являются одними из наиболее ценных видов деятельности, которые МАГАТЭ проводит в области компьютерной безопасности.

“При физической защите вы можете видеть, что вы защищаете, и представить себе вероятные варианты нападений, – говорит Дьюденхейффер. – А в киберпространстве у преступников появляется гораздо больше целей, в том числе цели вне установки; вы могли бы подвергнуться такому нападению даже дома. Мы должны научиться думать так, как думает преступник, чтобы лучше понять, как защищаться от кибератак, где мы ни находились”.