УДК 372.862

АСПЕКТЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЭНЕРГЕТИКИ

Д. Я. Околот, аспирант, e-mail: dokolot@kantiana.ru

ФГБОУ ВО «Калининградский государственный технический университет»

В статье рассматривается подготовка специалистов в области информационной безопасности для энергетической отрасли. Акцентируется внимание на проблеме обеспечения безопасности энергетических объектов, обосновывается важность подготовленности специалистов для работы в этой сфере. Характеризуется профессиональная компетентность специалистов в области информационной безопасности для работы в сфере энергетики.

информационная безопасность, энергетика, подготовка специалистов, профессиональная компетентность

Термин "информационная безопасность" стал актуальным с развитием интернета, компьютерных сетей передачи данных и других коммуникаций. Виртуальный мир становится все более похожим на мир реальный: люди общаются посредством использования интернета, читают книги и просматривают мультимедиа материалы в режиме онлайн, покупают товары в интернет-магазинах и даже могут совершать преступления в этой сфере. А если есть киберпреступники, значит, должны быть и специалисты, которые занимаются безопасностью объектов в сети. Это специалисты по информационной безопасности.

Электроэнергетика представляет собой отрасль, которая требует особого внимания и соблюдения тщательности во всем, в том числе и в вопросах обеспечения информационной безопасности (ИБ) и защиты информации (ЗИ). Энергетические комплексы относятся к стратегическим отраслям, являются одними из важнейших инфраструктурных систем в государстве и, соответственно, требуют особых мер обеспечения информационной безопасности.

При обеспечении защиты объекта энергетического комплекса в первую очередь необходимо исключить несанкционированные воздействия на оборудование энергетики – команды и нарушение связи между подстанциями. Как показывает практика, в сфере энергетики используются общепризнанные механизмы обеспечения ИБ. Для защиты технологических сетей, как правило, специфические инструменты не применяются. Специфика защиты промышленных объектов заключается в том, что средства защиты ни в коем случае не должны повлиять на технологический процесс.

Информация об уязвимостях оборудования, применяемого для управления и контроля над процессом передачи электроэнергии, а также для предотвращения повреждения высоковольтного оборудования в аварийных ситуациях и используемых сетевых протоколах, может позволить злоумышленнику влиять на технологический процесс. Также важное значение имеет защита сетевого оборудования, на котором организована передача информации за периметр подстанции в диспетчерские центры, поскольку современные предприятия объединены в промышленные сети и в большинстве своем связаны с офисными сетями, а в некоторых случаях и с интернетом.

Вторым важным моментом является защита рабочих мест операторов и серверов от вредоносного программного обеспечения, запуска неразрешенных приложений и подключения неучтенных внешних накопителей и других устройств. И третьей задачей обеспечения должного уровня ИБ объектов энергетики является защита промышленных контроллеров от несанкционированного доступа к ним, изменения исполняемого в них кода и отправки на них некорректных команд.

Угрозы в энергетической сфере в последнее время связаны, в первую очередь, с сетевыми атаками и атаками на автоматизированные рабочие места (АРМы) пользователей. В последние несколько лет специалистам стало очевидно, что промышленные системы защищены довольно слабо, а непрерывно увеличивающееся количество хакерских атак яркое тому подтверждение.

Слабость защиты современных объектов энергетики хорошо демонстрируют технические аудиты, которые, как правило, показывают наличие следующих брешей в защите: отсутствие корректной сегментации промышленных и офисных сетей, использование слабых или «зашитых» паролей, применение слабых парольных политик, наличие у операторов лишних прав, применение несанкционированного ПО и периферийного оборудования, а также отсутствие ответственных за обеспечение ИБ.

Еще одна важная особенность, которая накладывает свой отпечаток на обеспечение ИБ в энергетике, – большая территориальная распределенность информационных систем энергетических компаний с необходимостью реализации централизованной политики безопасности. По этой причине реализуется большое количество проектов по построению подсистем централизованного управления теми или иными сегментами системы обеспечения информационной безопасности (СОИБ).

Многие предприятия, осознав важность организации системы информационной защиты для энергетических объектов, сегодня столкнулись с нехваткой квалифицированных специалистов в этой области [1].

Таким образом, можно сделать вывод, что энергетические комплексы принадлежат к числу стратегических отраслей государства и нуждаются в особых мерах обеспечения информационной безопасности. Если на рабочих местах в рабочих помещениях и офисах вполне достаточно стандартных средств обеспечения ИБ (антивирусная защита, ограничение прав доступа пользователей, технологии аутентификации и т. п.), то защита на технологических участках генерации энергии и доставки конечным пользователям нуждается в повышенном контроле.

Значимость информационной безопасности в энергетической сфере определяется последствиями реализации информационных киберугроз. Это может привести к необратимым последствиям и нанести не только материальный ущерб или удар по репутации энергетических компаний и ресурсоснабжающих организаций (РСО), но и прежде всего – вред здоровью граждан, подрыв экологии, нарушение инфраструктуры города или региона.

Статистика инцидентов по отраслям промышленности показывает, что энергетика – одна из наиболее опасных и подверженных угрозам отрасль (рисунок) [2].

С учетом особенностей энергетической сферы одной из важнейших задач подготовки будущих специалистов в области информационной безопасности является формирование профессиональной компетентности в сфере обеспечения кибербезопасности в критических системах и в первую очередь выработка практических навыков, которые остро необходимы с самого начала работы на важнейших объектах электроэнергетики.

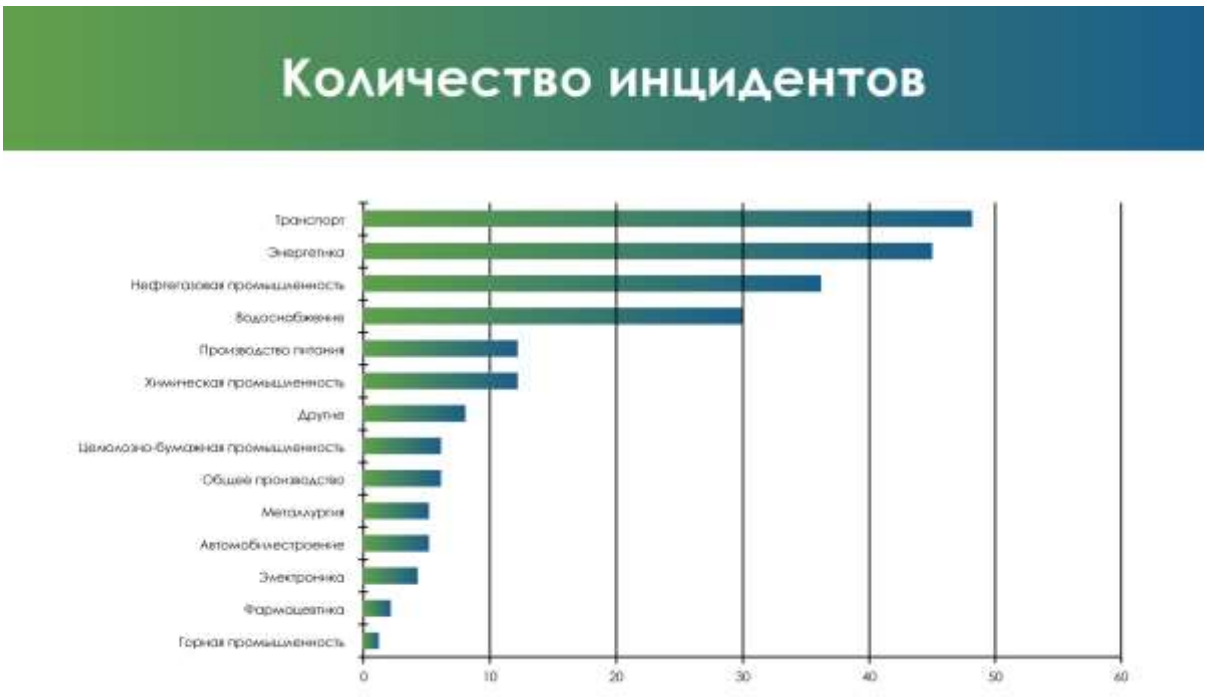

Рисунок – Количество инцидентов ИБ по отраслям промышленности

Следовательно, образовательная программа должна включать материалы, лежащие на стыке трех содержательных модулей: информационная безопасность, электроэнергетика и электротехника. На наш взгляд, в рамках подготовки студентов по этой программе основное внимание должно уделяться следующим вопросам:

• отличия обеспечения кибербезопасности современных промышленных систем от обеспечения информационной безопасности в системах общего назначения;

• особенности законодательной базы обеспечения кибербезопасности современных промышленных систем;

• уязвимости современных электроэнергетических систем, виды атак на них и способы противодействия этим атакам;

• организация и технологии эффективного функционирования центров управления инцидентами.

К составу и содержанию профессиональной компетентности специалиста по обеспечению ИБ в сфере энергетики также должны предъявляться специфические требования.

Согласно федеральным государственным стандартам группы 10.00.00 «Информационная безопасность» [4], в результате освоения программы обучения у выпускника должны быть сформированы универсальные (общекультурные), общепрофессиональные и профессиональные компетенции.

Как отмечают авторы [5], универсальные компетенции отражают общие требования, характерные для выпускника учебного заведения, независимо от области профессиональной деятельности. По нашему мнению, для специалиста по информационной безопасности в сфере энергетики наиболее важны такие универсальные компетенции, как способность мыслить аналитически, критически оценивать рабочие ситуации, принимать верное решение в таких ситуациях, аргументировано выстраивать личную позицию, осуществлять все виды коммуникаций в обществе и рабочем коллективе.

Общепрофессиональные компетенции представляются в виде совокупности основополагающих профессиональных способностей, знаний и умений специалиста, являющихся общими для осуществления любой профессиональной деятельности. К ним можно отнести общие практические навыки и умения, характерные для области

информационных технологий, такие как: ремонт и техническое обслуживание вычислительной техники, установка и настройка системного и прикладного программного обеспечения, оптимизация рабочих станций для максимальной производительности и т. п.

Профессиональные компетенции предполагают способность и готовность работника на основе усвоенных знаний, умений, приобретенного опыта, самостоятельно анализировать и практически решать профессиональные проблемы, типичные производственные задачи (проблемные ситуации), определяющие конкурентоспособность специалиста. К ним относятся: приобретение практических навыков с программными решениями в области обеспечения ИБ, развертывание, установка и настройка программного обеспечения на рабочих местах с целью обеспечения ИБ компании, получение документов установленного образца, подтверждающих наличие у специалиста таких навыков, и т. п. Профессиональные компетенции будущих специалистов в области ИБ должны соответствовать сфере его практической деятельности. При обеспечении ИБ объектов энергетики им потребуется знание не только технологий информационной защиты, перечня угроз и применения средств защиты с учётом их особенностей в энергетической отрасли и организациях этой отрасли, а также понимание правовых, инженерно-технических, организационных и других вопросов функционирования объектов энергетики.

Уровень сформированности профессиональной компетентности свидетельствует о том, насколько конкретный работник (выпускник образовательной организации) овладел своей специальностью, в какой мере он подготовлен к выполнению своих профессиональных обязанностей. Профессиональные компетенции отражают эффективность, безошибочность и быстроту принятия решения работником в этих проблемных производственных ситуациях.

По нашему мнению, необходимо заострять внимание студентов на том, что проектирование системы информационной защиты любого энергетического предприятия должно начинаться с прогнозирования и оценки рисков безопасности. Основной метод оценки – построение модели потенциальных угроз и модели нарушителя, которые помогут рационально распределять ресурсы при создании системы безопасности и предотвращать попытки реализации киберугроз. Кроме того, оценка рисков безопасности в энергетике отличается непрерывностью: аудит в процессе эксплуатации системы ведется непрерывно с целью выявления угроз, утечек и искажения данных, несанкционированного доступа к объектам энергетики и т. п., чтобы своевременно принимать меры по обеспечению максимальной степени защиты этих объектов и поддержания системы защиты в актуальном состоянии.

Также будущие специалисты должны понимать, что при разработке систем обеспечения ИБ или выборе средств защиты информации (СЗИ) для энергетических предприятий главным объектом защиты в энергетической сфере является не информация сама по себе, а технологический процесс производства и генерации энергии, являющийся источником и потребителем этой информации, а также доставка энергии ее потребителям. Система безопасности в таком случае должна обеспечить целостность технологического процесса и автоматизированных систем управления. Поэтому для эффективного применения и эксплуатации механизмов и технологий обеспечения информационной безопасности на предприятиях энергетического сектора, студенты должны в достаточной степени понимать устройство и функционирование таких объектов защиты, как:

- сам объект защиты – технологический процесс;
- средства и системы управления объектом (автоматика и телемеханика);
- системы, взаимодействующие с объектом (распределение электроэнергии, взаимодействие с потребителями, организационное управление и т. п.). В этом аспекте речь идет уже не о "привычной" защите от утечек информации, а о защите технологического процесса от реализации разнообразных киберугроз;
- сопутствующие факторы (релейная защита, автоматика, учет энергии). И речь в таком случае идет уже не о "привычной" защите от утечек информации, а о защите от нарушения технологического процесса за счет реализации киберугроз;

- организационно-управленческие подразделения предприятий в энергетике, в которых обращаются огромные объемы информации;
- системы передачи и хранения информации энергетической сферы;
- потребители энергии (которые могут в собственных интересах искажать передаваемую информацию о потреблении, что тоже может рассматриваться, как специфическая угроза).

Согласно [7], особенностью области энергетики является наличие двух уровней обеспечения ИБ:

- уровень корпоративных сетей и информационных систем;
- уровень АСУ ТП и технологических процессов в целом.

Следовательно, построение системы защиты должно осуществляться, исходя из базовых принципов ИБ: обеспечения целостности, конфиденциальности и доступности информационно-технологических объектов обоих уровней. При этом должна учитываться специфика АСУ ТП, используемых в энергетике (в том числе систем управления, телемеханики, релейной защиты и автоматики, коммерческого и технологического учета и т. д.).

Поскольку функционирование всех информационных систем энергетических компаний направлено на решение основной задачи – бесперебойной генерации и своевременной доставки электроэнергии конечным потребителям, то основными объектами защиты при обеспечении ИБ систем первого уровня являются:

- персональные данные (как сотрудников, так и клиентов);
- сведения об организации и функционировании критических инфраструктур;
- инсайдерская информация [7].

Соответственно в системе обеспечения ИБ энергетического предприятия должны быть выделены следующие уровни:

- физической безопасности (ограничение физического доступа к панелям управления, диспетчерским и другим помещениям, устройствам, кабелям) с целью исключить несанкционированный доступ;

- сетевой безопасности – в него входят сетевая инфраструктура офиса компании (например, межсетевые экраны со встроенными сенсорами систем предотвращения вторжения) и средства защиты, интегрированные в сетевое оборудование (коммутаторы и маршрутизаторы);

- безопасности рабочих станций и серверов (управление обновлениями ПО, применение антивирусного ПО, удаление неиспользуемых приложений, протоколов и сервисов);

- безопасности приложений (аутентификация, авторизация и аудит при доступе к приложениям);

- безопасности устройств (контроль над изменениями и ограничение доступа).

На основании всего изложенного можно сделать вывод, что подготовка специалистов по информационной безопасности для предприятий энергетической сферы должна в значительной степени учитывать отраслевую специфику. Для обеспечения должной эффективности образовательного процесса на всех его этапах должно осуществляться тесное взаимодействие профессионалов в области энергетики, информационной безопасности и педагогики профессионального образования.

СПИСОК ЛИТЕРАТУРЫ

1. АИС провела первый мастер-класс в рамках Центра компетенции ИБ АСУ ТП компании ICL СТ. 2018 год. [Электронный ресурс]. Режим доступа: http://www.icl.ru/press-center/news/ais-held-the-first-master-class-within-the-framework-of-the-competence-center-of-information-securit/

2. Мелких, А. А. Исследование проблемы информационной безопасности АСКУЭ / А. А. Мелких, С. Ю. Микова, В. С. Оладько // Universum: Технические науки. – 2016 г.

3. Невский, А. Без погон, но офицеры. 2013 год. [Электронный ресурс]. – Режим доступа: https://journal.ib-bank.ru/post/239

4. Федеральные государственные образовательные стандарты среднего профессионального образования (ФГОС СПО) нового поколения. 2018 год. [Электронный ресурс]. – URL: http://www.edu.ru/abitur/act.86/index.php#Par10 Режим доступа: свободный.

5. Компетенция. Компетентность. Компетентностный подход / под ред. доктора пед. наук, профессора И. Д. Рудинского. – Москва: Горячая линия – Телеком, 2018. – 240 с.

6. Информационная безопасность в энергетике. 2018 год. [Электронный ресурс]. – URL: http://systemres.ru/security/ib_energy_sector/

7. Прохоров, Д. Информационная безопасность в электроэнергетике. Отраслевые нюансы / Д. Прохоров, А. Кондратенко // «Connect! Мир связи». – 2012. – № 3. – С. 32-34.

THE ASPECTS OF TRAINING SPECIALISTS FOR ENSURING INFORMATION SECURITY IN THE SPHERE OF ENERGY

D. Y. Okolot, PhD student
dokolot@kantiana.ru
Kaliningrad State Technical University

In the article considers the training of specialists in the field of information security for the energy industry. The attention is focused on the problem of ensuring the safety of energy facilities, the importance of the preparedness of specialists for work in this area is substantiated. Characterized by the professional competence of specialists in the field of information security for work in the energy sector.

information security, energetics, training of specialists, professional competence