УДК 004

Козлова И. С.
асс.,
Дьячкова В. В.
к.э.н., доц.
Донбасский государственный технический университет, г. Алчевск, ЛНР, Россия

О БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Современное общество представляет собой многогранный организм, состоящий из множества разнообразных средств и систем, его обслуживающих. Эти системы и средства настолько тесно переплетены между собой, что возникает понятие инфраструктуры, т. е. совокупности различных служб, систем, сооружений, которые важны для нормального функционирования экономики и обеспечения благополучной повседневной жизни населения. Зачастую сбои в работе одной системы неуклонно ведут к сбоям работы другой или же всех систем сразу. К критической же инфраструктуре относятся фундаментальные средства и системы, обслуживающие страну и обеспечивающие ее национальную безопасность.

Критическая инфраструктура (КИ) обеспечивает успешную работу важных для существования государства и жизнеобеспечения общества служб и систем: органов власти, водоснабжения, финансовых и налоговых систем, космических технологий, крупных промышленных предприятий, добычи полезных ископаемых, электростанций в т. ч. атомных, транспортного обеспечения, телекоммуникаций и др. В состав такой инфраструктуры входят самые разнообразные ресурсы, услуги и объекты, повреждение или разрушение которых может серьезно отразиться на здоровье, безопасности, экономическом благополучии населения или государства. Поэтому вопрос обеспечения безопасной и бесперебойной работы всех составляющих критической инфраструктуры крайне важен для любого сообщества.

Работа критической инфраструктуры может быть нарушена как преднамеренными террористическими актами, преступными действиями, взломами компьютеров, так и непредсказуемыми экзогенными воздействиями (стихийными катастрофами, авариями). Для сохранения неприкосновенности жизни и имущества граждан, действия над КИ должны быть редкими, краткими, управляемыми, географически изолированными и с минимальным ущербом.

Безопасность критической инфраструктуры, в первую очередь, направлена на устранение уязвимостей этих структур и предотвращение саботажа и терроризма. В настоящее время наблюдается широкое внедрение современных компьютерных технологий для автоматизации многих трудоемких процессов. Критические инфраструктуры также не избежали этого явления. В результате они стали очень взаимосвязанными и взаимозависимыми.

История угроз и масштабных атак на критические инфраструктуры в последние годы все больше связана с IT-системами, которые обеспечивают их деятельность, например [1]:

– 1999 г. — зафиксированы нарушения в работе систем безопасности российского гиганта «Газпром». При помощи инсайдера был внедрен троян для контроля за подачей газа;

– 2002 г. — в Венесуэле подверглась атаке нефтяная компания PDVSA, произошло сокращение добычи нефти и взломано несколько корпоративных компьютеров;

– 2008 г. — в Польше, г. Лодзь студент взломал системы трамвайной сети, что привело к схождению с путей 4 трамваев, а 12 человек получили травмы;

– 2012 г. — нефтяная компания Saudi Aramco подверглась атаке хакеров, в результате они получили доступ к 30000 корпоративным компьютерам;

– 2014 г. — зафиксирована атака на одном из металлургических заводов в Германии. Результатом стала невозможность отключения одной из домен, что принесло огромный ущерб предприятию;

– 2015 г. — национальная электросеть Украины подверглась кибер-атаке, в итоге более 600000 жителей страны остались без электричества.

И это лишь небольшое число примеров, такие атаки с каждым днем увеличиваются в количестве и своем негативном воздействии на жизнь общества.

Как видим, критические инфраструктуры становятся все более и более зависимыми от информационных коммуникационных технологий, поэтому защита этих систем требует разработки решений, которые учитывают уязвимости и проблемы безопасности, обнаруженные в этих технологиях.

Защита критической инфраструктуры включает в себя совместные мероприятия владельцев инфраструктуры, операторов и регулирующих органов, которые направлены на поддержание критически важных объекты инфраструктуры в случае сбоев, атак или аварий. Безопасность критической инфраструктуры индивидуальна для каждой системы. Не существует одного стандартного решения, позволяющего обеспечить безопасность всех критических инфраструктур. Но для создания системы по обеспечению безопасности КИ можно выделить следующие основные этапы, которые будут характерны для любой инфраструктуры [2]:

1) определение возможных угроз и необходимость создания системы безопасности;

2) непосредственное создание системы безопасности;

3) планирование, при котором устанавливаются требования, необходимые для обеспечения безопасности при возможных угрозах и составляется план мероприятий;

4) реализация — происходит внедрение организационных и технических мер, по осуществлению плана мероприятий для обеспечения безопасности;

5) мониторинг и контроль деятельности системы безопасности, выявление узких мест;

6) совершенствование, которое предполагает, что система защиты должна противодействовать угрозам не только сегодня, но и в будущем, процессы и мероприятия по защите должны перманентно совершенствоваться и повышать свою зрелость.

Развитие экономики, технологий и общества в целом не стоит на месте, поэтому для успешного функционирования в безопасном режиме этапы 3–6 постоянно повторяются.

Используемые в КИ IT-системы состоят из всевозможных гетерогенных компонентов и разнообразных технологий. Эти системы имеют множество проблем безопасности, что делает критическую инфраструктуру уязвимой для атак.

Невозможно знать и предугадать, какая информация доступна кибер-преступникам и какие технические средства находятся в их распоряжении, поэтому мы не можем ответить на вопрос, насколько обеспечена сейчас безопасность объектов критической инфраструктуры. Но всегда есть возможность улучшить защиту от уже известных атак и принимать меры по их предотвращению. Это проверка систем на уязвимости, особенно в тех случаях, когда уже были зафиксированы и существовали некоторое время дыры; мониторинг систем, используемых для контроля критической инфраструктуры, и в случае необходимости их полная изоляция от внешних соединений, что позволит обнаруживать внешние атаки и предотвращать доступ к системам, управляемым из внутренней сети; контроль над съемными устройствами, которые могут служить как источником вредоносного ПО так и для кражи конфиденциальной информации; мониторинг ПК, к которым подключены программируемые логические контроллеры (PLC), так как они подключены к Интернету и могут предоставлять хакерам доступ к критически важным системам управления.

Список литературы

1. Самые громкие кибер-атаки на критические инфраструктуры [Электронный ресурс] // pcnews : [сайт]. URL: https://pcnews.ru/blogs/samye_gromkie_kiber_ataki_na_kriticeskie_infrastruktury-738949.html#gsc.tab=0.

2. Безопасность объектов критической информационной инфраструктуры организации. Общие рекомендации (версия 2.0). М. : АРСИБ, 2019. URL: http://aciso.ru/files/docs/metodichka_2.0.pdf?ysclid=lhgd4pm4nj17012561.