М.Д. КРАСНИЦКИЙ,
руководитель проектов
ООО «МультиТек Инжиниринг»

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ

Электроэнергетика, как и многие другие отрасли экономики, активно движется по пути цифровизации. Однако, наряду с очевидными преимуществами, цифровизация сопряжена с рисками для информационной безопасности (ИБ). Привычным явлением современности стали кибератаки. При этом компании и объекты, которые подвергаются таким атакам, не всегда имеют эффективную защиту и в результате несут значительные убытки.

Кибератаки и их последствия

С каждым годом число кибератак в мире растет. Так, корпоративные сети крупных компаний, в том числе энергетических, и государственных учреждений по всему миру были атакованы с использованием вируса Petya, ущерб от которых оценивается более чем в $ 10 млрд.

Вирус Stuxnet успел заразить около 200 тыс. электронных устройств. Особенно пострадала ядерная программа Ирана, где кибератака вывела из строя более тысячи центрифуг для обогащения урана.

Сетевой вирус Win32/Stuxnet поразил персональные компьютеры, а также АСУ ТП. Он позволил злоумышленникам перехватить и изменить поток данных промышленных предприятий, электростанций и аэропортов.

Серия кибератак на крупные промышленные предприятия Германии была совершена с помощью вируса Havex. Чтобы получить доступ к корпоративным сетям предприятий, злоумышленники атаковали их сайты, используя методы социальной инженерии и фишинга. Проникая в сети, непосредственно контролирующие технологический процесс, преступники нанесли огромный ущерб промышленному оборудованию.

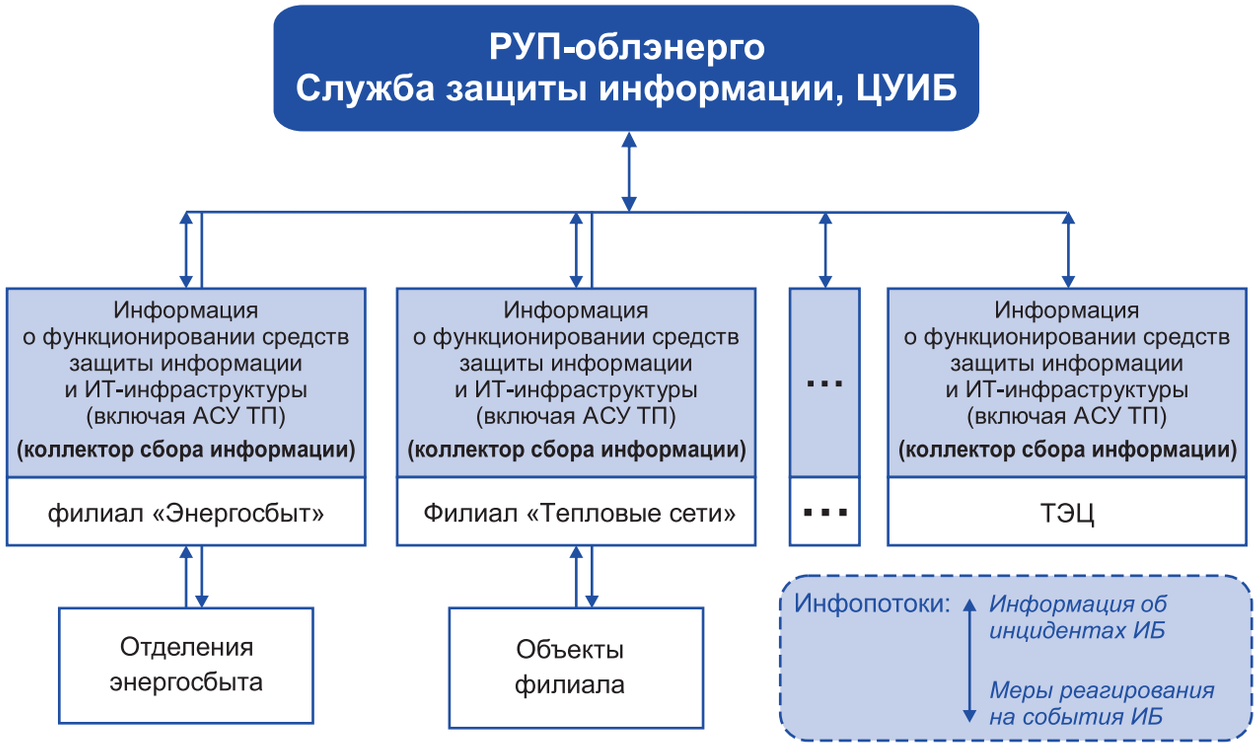
Вирус WannaCry успел заразить более полумиллиона компьютеров в 150 странах мира и нанести ущерб около $ 1 млрд. Вирус зашифровывал все содержимое компьютера, а затем начинал требовать деньги за разблокировку. Однако даже после уплаты выкупа файлы не восстанавливались. В результате банки, правительственные организации, аэропорты, учреждения здравоохранения и т.д. вынуждены были останавливать работу

Крупнейший оператор трубопроводов в США подвергся кибератаке программы-вымогателя DarkSide. Из-за остановки трубопровода Министерство транспорта США объявило чрезвычайное положение в нескольких штатах, оптовые цены на бензин в США повысились, возникли перебои с топливом на автозаправках. Выкуп составил более $ 4 млн.

Особый риск кибератаки несут для объектов электроэнергетики. Решение задачи обеспечения информационной безопасности в этом случае осложняется целым рядом факторов, наиболее существенными из которых являются следующие:

- территориальная распределенность электроэнергетических предприятий;
- отсутствие необходимого количества квалифицированных специалистов по ИБ;
- опасность деструктивного вмешательства в технологические процессы при внедрении средств защиты информации;
- высокие капитальные затраты на покупку и внедрение средств защиты информации наряду с высокими эксплуатационными расходами;
- отсутствие у задачи конечного срока решения, поскольку абсолютной защиты не бывает и вопросы обеспечения ИБ требуют непрерывного внимания.

Существует множество разнообразных угроз безопасности информации электроэнергетического предприятия: от вмешательства извне или изнутри в работу или в каналы связи управляющих устройств с конечными физическими устройствами (оборудование генерации, распределения и учета, контрол-



Пример информационной схемы ЦУИБ РУП-облэнерго

леры и пр.) до фишинговых писем или интернет-ссылок. Поэтому обеспечение ИБ – задача комплексная, ее решение затрагивает все подразделения предприятия, требует воли и решимости руководства, затрат на разработку и внедрение средств обеспечения ИБ, а также вовлеченности персонала.

Рекомендуемый подход к организации информационной безопасности

Предлагаем пошаговый подход к организации информационной безопасности для условного областного предприятия электроэнергетики (РУП-облэнерго) с входящими в его структуру аппаратом управления, генерирующими и распределительными предприятиями и их филиалами. Организации системы ИБ включает:

1. Создание службы защиты информации.

2. Проектирование, создание и внедрение типовых решений по защите информации.

3. Внедрение в службе защиты информации процессов централизованного мониторинга и реагирования на инциденты ИБ на базе программно-аппаратного центра управления информационной безопасностью (ЦУИБ), с которым интегрируются типовые решения.

4. Поддержка службой защиты информации динамичного и непрерывного процесса обеспечения ИБ.

Шаг первый. В РУП-облэнерго создается служба защиты информации (подразделение по защите информации), подчиненная первому руководителю или его заместителю, не курирующему службу ИТ. Служба наделяется соответствующими полномочиями: разрабатывает и внедряет систему менеджмента ИБ, занимается проектированием, созданием, внедрением и эксплуатацией систем защиты информации (самостоятельно и/или с привлечением специализированных организаций). В целях сокращения материальных и людских затрат на обеспечение и поддержание процессов ИБ служба ориентируется на использование программно-технических средств, обеспечивающих централизацию управления ИБ в РУП-облэнерго.

Централизация управления ИБ позволит сконцентрировать организационные, методологические и технологические вопросы обеспечения защиты информации РУП-облэнерго в едином центре.

Шаг второй. Подразделение по защите информации разрабатывает и внедряет типовые решения по обеспечению ИБ на объектах РУП-облэнерго (процессы, регламенты, технологии, средства, способы и методы взаимодействия в системе защиты информации). Требования к ИБ в заданиях на проектирование (модернизацию) объектов электроэнергетики и разработку информационных систем, автоматизирующих производственную деятельность РУП-облэнерго, должны формироваться с учетом типовых решений и согласовываться со службой защиты информации, а приемка работ по проектированию и строительству объектов должна осуществляться с участием специалистов данной службы.

Шаг третий. Подразделение по защите информации обеспечивает автоматизацию управления ИБ посредством внедрения ЦУИБ. Данные о событиях ИБ формируются средствами защиты информации в корпоративном и технологическом сегментах сети РУП-облэнерго. При этом могут иметь место и ложноположительные сигналы, значительно увеличивающие общий информационный поток. Для того чтобы персонал службы защиты мог справиться с потенциальным информационным «валом», в ЦУИБ размещается система сбора, обработки и анализа событий из различных источников, позволяющая выявлять и ранжировать инциденты ИБ в зависимости от степени их влияния на функционирование РУП-облэнерго. Коллекторы этой системы, выполняющие сбор данных и их передачу в ЦУИБ, располагаются в филиалах (см. рисунок).

Но это – лишь часть процесса обеспечения ИБ. После обнаружения инцидентов ИБ необходимо быстро (иногда счет идет на минуты) определить их критичность, согласовать и реализовать решения и меры по устранению возникших или предотвращению потенциальных угроз. Однако оперативности действий персонала мешают как сложность выбора мер, так и их медленное согласование, обусловленное человеческим фактором. Решением проблемы является автоматизация управления процессами реагирования, позволяющая не только значительно сократить время реакции и повысить ее эффективность, но и предоставляющая специалистам службы защиты информации возможность расследовать действительно важные инциденты, не отвлекаясь на рутинные действия.

Именно интеграция в рамках ЦУИБ процессов сбора и анализа событий ИБ и автоматического реагирования на инциденты ИБ позволит создать эффективную систему защиты информации для всех предприятий РУП-облэнерго. При этом средства защиты будут находиться «на местах», а сбор и анализ информации, оперативная выработка мер реагирования и их контроль – осуществляться в ЦУИБ.

Таким образом, служба защиты информации РУП-облэнерго может обеспечивать из единого центра:

- анализ на уязвимости и защиту от целенаправленных кибератак корпоративной и технологической сетей аппарата управления и филиалов;
- автоматизированный сбор информации о событиях ИБ с источников – средств защиты информации, оборудования и ПО локальных вычислительных сетей аппарата управления и энергообъектов;
- автоматизированный анализ событий и выявление инцидентов ИБ;
- организацию и автоматизацию работы по реагированию на инциденты, их расследованию, планированию мероприятий по недопущению повторения подобных инцидентов, контролю за выполнением этих мероприятий;
- автоматизированный контроль за работой привилегированных пользователей корпоративной сети РУП-облэнерго;
- автоматизацию обучения и тренировки навыков в области ИБ пользователей корпоративной и технологической сетей.

Программные и технические средства управления ИБ имеют достаточно высокую стоимость, и для их эксплуатации требуются квалифицированные специалисты по ИБ. Поэтому сосредоточение этих средств в ЦУИБ и использование в интересах всех предприятий РУП-облэнерго позволит, во-первых, сократить эксплуатационные расходы, а во-вторых – сконцентрировать дефицитные кадры в едином центре, за счет этого уменьшив потребность в них на местах.

Параллельно с внедрением средств защиты информации на предприятиях РУП-облэнерго должно проводиться обучение оперативного персонала правилам поведения (порядку действий) в случае наступления инцидентов ИБ.

Шаг четвертый. Служба защиты информации РУП-облэнерго, используя программно-технические компоненты, на постоянной основе обеспечивает:

- непрерывный контроль за состоянием ИБ (аудиты, анализ угроз, оценка рисков);
- планирование развития и модернизацию системы защиты информации,
- обучение своих специалистов и пользователей информационных систем.

Подобный подход к организации ИБ на предприятиях электроэнергетики достаточно хорошо апробирован в России и активно внедряется в практику. В РФ разработаны технологии создания и развития ситуационных центров, программы подготовки кадров службы защиты информации, формы соглашения об уровне предлагаемых службой ИБ-сервисов, необходимая организационно-распорядительная документация и др.

Защита информации электроэнергетического предприятия – это перманентный процесс, позволяющий при правильных подходах предотвратить кибератаку, а в случае невозможности ее предотвращения – минимизировать возможный ущерб и в приемлемые сроки восстановить нормальную производственную деятельность.

По нашему мнению, реализация вышеуказанной программы действий позволит РУП-облэнерго обеспечить информационную безопасность производственных процессов, использующих цифровые технологии.