Охрана предприятия

№9

Оглавление

Книжное обозрение

Safety and Security Issues in Electric Power Industry
Zdzisław Żurakowski

Исследования

Кризис и информационные утечки: риски растут, меры противодействия ужесточаются

Цена аварий на энергетических объектах за 100 лет

В журнале Energy Policy за май прошлого года был опубликован исследовательский отчет об авариях, случившихся в мире с 1907 по 2007 год. Были изучены обстоятельства и последствия 279 крупных аварий на тепловых, ядерных и гидростанциях.

Отбор фактов проводился по следующим критериям:
- аварии, произошедшие в любой цепи энергетической системы (производство, передача, распределение энергии);
- последствия с человеческими жертвами и/или материальным ущербом свыше $50, 000 (в ценах 2006 года);
- аварии на гражданских объектах и в мирное время;
- период с августа 1907 г. по август 2007 г.;
- наличие публикаций, подтверждающих факт аварий.

Исследование показало, что аварии на гидросооружениях, занимающие всего 1% от общего числа инцидентов на энергетических объектах, обернулись наибольшим уроном – 94% человеческих жертв. Правда, следует отметить, что прорыв плотины Шимантан (Китай) в 1975 году унес сразу 171 000 человеческих жизней.

На втором месте по числу жертв – аварии на атомных станциях. Они же нанесли наибольший материальный ущерб (41% экономических потерь). Затем по этому показателю идут ГЭС и тепловые станции, использующие нефть (по 25%), натуральный газ (9%), и уголь(2%).

Чаще всего из строя выходят энергетические объекты, работающие на газе, затем по степени убывания идут станции, использующие нефть, атомную энергию, уголь и на последнем месте – ГЭС.

Аварии на энергообъектах происходят так часто, что уже давно стали восприниматься как рутина, за исключением наиболее серьезных, тяжелых по своим последствиям, отмечается в отчете. Поэтому им уделяется так мало внимания с точки зрения внедрения и использования новейших технологий, несмотря на заметные улучшения в

проектировании, строительстве, управлении и эксплуатации.

Частая повторяемость аварий позволяет заранее их предвидеть, а, следовательно, заблаговременно готовиться к ликвидации последствий, тем самым сводить к минимуму потенциальный урон.

(по материалам сайта scitizen.com)

Безопасность ГЭС и плотин в национальной стратегии США

В официальных документах правительства США плотины и ГЭС входят в число пяти приоритетных с точки зрения национальной безопасности категорий стратегических объектов.

Из примерно 77 тысяч плотин в ведении федерального правительства находятся только 5%. Это крупные гидросооружения, аварии и другие чрезвычайные ситуации на которых чреваты наибольшим человеческим и материальным уроном. Остальные объекты принадлежат местным властям, коммунальным компаниям, корпоративным или частным владельцам. Разнообразие форм собственности затрудняет применение универсальных стандартов безопасности и контроль.

Национальная стратегия США формулирует 6 основных путей, по которым строится политика поддержания и укрепления защиты плотин и ГЭС.

1. Развитие и внедрение современных методологий оценки рисков.

2. Разработка планов и мер по защите наиболее важных гидрообъектов (в рамках специальной группы Министерства внутренних дел).

2. Сбор и распространение среди менеджмента и владельцев гидросооружений важной информации по обеспечению безопасности объектов (через специально созданный на федеральном уровне Информационно-аналитический Центр).

3. Создание национальной программы по обеспечению безопасности гидросооружений.

4. Разработка защитных мер в чрезвычайных ситуациях.

5. Развитие технологий безопасности применительно к защите гидрообъектов.

(по материалам сайта fema.gov)

Проблемы обеспечения безопасности

на электростанциях США

Современная система обеспечения безопасности на американских электростанциях, по мнению экспертов (Александр Фаррел, Лестер Лейв, Гренджер Морган), способна успешно противостоять природным катаклизмам (землетрясения, ураганы и т.п.), но не приспособлена к стопроцентной защите от хорошо организованных нападений террористов и кибер-атак. Поэтому, как они считают, «стратегия обычной защиты» электростанций уходит в прошлое, на смену приходит «стратегия выживания». Вместо того, чтобы ломать голову над превращением энергетических объектов в «неприступные крепости», надо вести дело к созданию такой системы безопасности, когда выход из строя одного, пусть даже важного компонента, не приведет к полной остановке электростанции, но позволит ей продолжать функционировать, хотя бы в ограниченном масштабе, и затем быстро восстановить все мощности (issues.org).

Анализ аварий, временных отключений от электричества городов и целых регионов Америки, привел к выводу о ключевом значении следующих факторов выживания:

- заблаговременная разработка планов действий в экстремальных условиях;

- наличие достаточных объемов и ассортимента запасных частей;

- учебная подготовка персонала к работе в чрезвычайной ситуации.

- создание надежной системы коммуникации, способной работать в условиях тяжелейших аварий.

- организация информзащиты.

Одна из проблем, с которыми сталкиваются энергетические предприятия США - невозможность привлечь серьезные частные инвестиции на дорогостоящие проекты для усиления их охраны и безопасности. Акционерам такого рода вложения представляются малоинтересными, поскольку не сулят быстрой и реальной прибыли. По этой причине упомянутые выше эксперты считают критически важной роль государства, правительственных органов в решении таких задач.

Надо отметить, что после крупнейшей аварии 9 ноября 1965, в результате которой сначала отключился район г. Нью-Йорка, а затем "затемнение" распространилось на весь Северо-Восток США, американское правительство отреагировало созданием Северо-американского совета по обеспечению электроснабжения (NERC), которое устанавливает стандарты надежности и контролирует их выполнение всеми энергетическими предприятиями региона. Конечно, и этот федеральный орган не смог предотвратить крупнейшие аварии 1973, 1977, 2003 годов в северных штатах Америки (кстати, последние две случились в августе месяце, считающемся в России «черным»).

Проблем добавили информационные инновации. Сегодня многие системы управления и контроля в энергетической сфере базируются на Интернет-технологиях. Между тем, и правоохранительные органы США, и частные охранные предприятия заявляют о ненадежности информационной защиты энергообъектов – она легко преодолима извне. Но кто должен заниматься усилением этой защиты: сами компании или государство? Вопрос о разделении полномочий до конца не ясен. Экспертам ясно, без государственной поддержки не обойтись: акционеры не хотят вкладываться

обеспечение безопасности.

Еще один вывод, к которому склоняется все больше специалистов – это отказ от крупных энергетических предприятий в пользу сетей мелких компаний. Наличие последних локализует последствия техногенных аварий, равно как и террористических актов, и кибер-атак.

готовые строительные фирмы

Спасти людей во время пожара на ГЭС

Принято считать, что для гидроэлектростанций пожары не представляют серьезной опасности. Это не так, утверждает главный инженер по противопожарной безопасности компании Starr Technical Risks Agency Inc. Доминик Диекен. Более того, пишет он в статье на сайте powermag.com, в некоторых отношениях опасность там даже серьезнее, чем на тепловых станциях. Эксперт имеет в виду американские гидроэлектростанции, возраст которых весьма почтенный – от 30 до 70 лет.

Известны случаи крупных пожаров на гидроэлектростанциях многих стран, причинивших немалый урон: Швейцария (1996 г.), США (1981 и 1982 гг), Португалия (1997 г)...

Основные риски связаны с эксплуатацией наполненных маслом трансформаторов, электрических кабелей, распределительных устройств, систем кондиционирования. Что отличает в худшую сторону гидростанции от тепловых – то, что значительная часть служебных помещений находится ниже уровня выпуска воды. А это значит, что в случае серьезной аварии, пожара возможности для быстрой эвакуации персонала ограничены. Поэтому при строительстве и во время эксплуатации гидроузлов особое внимание уделяется вопросам безопасности работающих там людей. В статье Д. Диекена рассматриваются основные требования противопожарной безопасности для ГЭС. Они отражены в разных официальных документах, включая «Свод правил по безопасности людей» Национальной ассоциации по защите от пожаров (NFPA).

Выходы и расстояния

В требованиях к проекту гидроэлектростанций записано, что максимальное расстояние от рабочего места до выхода наружу или в безопасное помещение не должно превышать 100 метров, длина общего коридора – не более 15 метров, и максимум 15 метров – для тупичков.

Запасные (пожарные) выходы

Каждый уровень станции должен иметь два пожарных выхода. Правила допускают и использование настенных лестниц (трапов) – там, где они уместны. Большие гидроэлектростанции (с числом уровней более 2) обязательно должны предусматривать минимум две пожарные лестницы.

Административные помещения

Административные помещения (дирекция, бухгалтерия, отдел кадров, вспомогательные службы) не должны напрямую соединяться с основными

производственными помещениями. Они должны иметь отдельные, собственные выходы на общие лестницы, свои пожарные выходы.

Тревожная сигнализация

«Свод правил» требует установку пожарной сигнализации на ГЭС с численностью персонала 100 и более человек, но в реальности все без исключения гидроэнергетические объекты имеют такие системы.

Аварийное освещение

Аварийное освещение при отказе работы ГЭС необходимо. Исключение составляют небольшие объекты, работающие в автоматическом режиме, где персонал используется время от времени – для проверки и отладки оборудования. Аварийное освещение предназначено не для всего сооружения, но только для лестниц, коридоров, проходов, пандусов.

Для работы в некоторых рабочих помещениях правила требуют обязательное наличие ручных фонарей. Известен случай, когда контролер благодаря такому фонарю смог предотвратить ущерб от начавшегося пожара.

Аудит безопасности – путь к снижению рисков при эксплуатации ГЭС

Канадский журнал Canadian Security Magazine (canadiansecuritymag.com) в марте прошлого года опубликовал статью Дженнифера Брауна, посвященную вопросам охраны и безопасности гидростанций.

Ключевым моментом в проведении политики безопасности, направленной на снижение рисков, автор статьи считает «разработку и осуществление плана проверок, как исполняются требования и стандарты безопасности». Он рассказывает о реализации такого плана на примере канадской компании B.C. Hydro, которая управляет несколькими десятками гидрообъектов и двумя тепловыми станциями. .

Браун пишет, что в прошлом оценка рисков осуществлялась с помощью ручки и бумаги. Сегодня на смену пришли новые технологии, конкретно – софтовые программы D3 Security Management Systems и Asvaco Threat Risk Assessment, которые разработаны на основе принятых в США и Канаде стандартов безопасности американского Федерального агентства по управлению чрезвычайными ситуациями (Federal Emergency Management Agency). Конечно, компания могла бы разработать собственный программный продукт, который бы учитывал наряду с общими стандартами специфические особенности своих объектов, но это заняло бы несколько лет.

B.C. Hydro использует программы для оценки четырех степеней рисков. Первая степень, самая простая, охватывает риски для небольших зданий с двумя-тремя помещениями внутри, которые не представляют особой опасности. Вторая, третья и особенно четвертая степени предусматривают всевозможные сценарии возникновения

чрезвычайных ситуаций применительно к более сложным объектам, включая нападения террористов. «Например, программы помогают виртуально проникнуть в возможные замыслы потенциальных преступников, представить подробную картину их вероятных действий во время нападения. Это важный антитеррористический компонент, позволяющий предвидеть и принимать необходимые меры защиты».

В 2007 и 2008 годах с помощью компьютерных технологий была проведена оценка рисков более двух третей всех объектов. Полностью такая работа будет закончена к концу 2009 года. Затем будет разработан и введен в действие план усиления охраны и безопасности, который охватит всю сеть энергетических станций.

Главный выигрыш такой методологии заключается в стандартизированном подходе к оценке рисков, независимо от того, какой объект изучается, насколько он сложный в эксплуатации, насколько он важен для энерго-системы. Такой стандартизированный подход к оценке рисков и мерам по защите особенно важен в энергетической отрасли, которая включает в себя объекты разной сложности и функциональности. «Он дает управляющему менеджменту возможность определить не только, какие риски имеются в компании, но где именно и какой специфики».

Кибер-угрозы и меры защиты электроэнергетики

Выдержки из выступления в Конгрессе директора лаборатории информационных технологий Национального института стандартов при Министерстве торговли США Ч. Фурлани

Для повышения надежности работы электроэнергетики критически важное значение имеет как физическая, так и информационная защита. С учетом перевода работы и взаимодействия между энергетическими компаниями на Интернет-технологии, угрозы кибер-атак возрастают. Существующие информационные бреши позволяют потенциальному злоумышленнику вторгнуться в компьютерные коммуникации, получить доступ к контрольным программным продуктам, создать условия, ведущие к дестабилизации электросетей.

Среди дополнительных рисков:

- растущие сложность, громоздкость систем электроэнергии чреваты появлением новых уязвимостей, фатальными ошибками и преступными вторжениями;

- развитие коммуникации между компьютерными сетями разных компаний создает общие для них уязвимости и слабости;

- эти уязвимости могут привести к отказу или сбоям в работе программ и систем;

- увеличением числа входов в компьютерные сети могут воспользоваться преступники;

- растет угроза взлома баз конфиденциальных данных, включая приватную информацию клиентов энергетических компаний;

- увеличивается риск физических атак.

Предварительный перечень защитных мер, которые содержатся в докладе, в частности, предполагает:

- организовать на должном уровне физическую охрану и информационную защиту корпоративных баз данных;

- предусмотреть, чтобы любая модификация данных и командных установок немедленно фиксировалась;

- соблюдать режим конфиденциальности в работе с информацией, включая системы персональной идентификации;

- предусмотреть меры, исключающие отказ всей энергетической системы в случае преднамеренных нападений, случайных ошибок, стихийных бедствий;

- обеспечить наличие техники и технологий, необходимых для быстрого восстановления поврежденных сетей и энерго-объектов;

- проводить регулярный аудит безопасности;

- обеспечить охрану всей цепи энерго-поставок, дабы не допустить сбоев в отдельных звеньях.

Новые коммуникационные технологии будут более защищенными и безопасными

С появлением и бурным развитием в последние десятилетия новых информационных технологий совершенно изменился характер внутрикорпоративных связей и внешних коммуникаций с партнерами, поставщиками, клиентами. Время и расстояния перестали служить барьером к развитию производства и повышению эффективности экономики.

Вместе с тем, возникли новые угрозы и риски. Пользование электронной почтой для служебной переписки, рассылки корпоративных документов и других целей на деле означает, что значительные массивы информации в процессе передачи реально оказываются вне контроля. Проблема весьма серьезна. Проведенный исследовательской фирмой KRC Research опрос показал, что практически в каждой второй американской компании сотрудники пользуются услугами коммуникационных посредников для электронной переписки с партнерами. Причем характер информации весьма широк и напрямую затрагивает вопросы безопасности бизнеса. Это и производственные планы, и технические данные, и ценовые установки, и деловые контракты..... «Трудно представить, какой огромный урон может быть причинен компании, - пишет Тайлер Брайсон из Microsoft, - если такая информация окажется в

руках конкурентов, что в принципе нельзя исключать при широком использовании коммуникационными услугами третьей стороны» (Industryweek.com).

Понимают ли бизнесмены риски, которым они подвергаются? Скорее всего, понимают, но в современной экономике, где скорость принятия решений, передачи информации играет возрастающую роль, риск опоздать представляется им большим злом по сравнению с угрозой информационной утечки.

Однако, отмечает Брайсон, находящие в разработке коммуникационные инновации обещают решение этой дилеммы. Они призваны обеспечить сочетание скорости в передаче данных с их безопасностью, полностью контролируя весь процесс: кому информация предназначена, как и где найти адресат, что делать, если адресат вне зоны досягаемости.

Новые умные программные решения предусмотрят плавное переключение с одного вида связи на другой по тем или иным обстоятельствам: например, сообщение, которое стартует в электронном виде (e-mail), может автоматически преобразиться в голосовое сообщение, передаваемое на мобильный телефон, а затем в том же режиме стать частью видеоконференции.

Видеоконференции вообще получат совершенно новое качество. Голография и другие инновации позволят создавать полное ощущение происходящего в едином замкнутом пространстве, даже если участники события находятся по разные стороны света.

Одно из важных новшеств: каждый индивид сможет иметь единую цифровую идентичность для всех видов коммуникации. Программный продукт самостоятельно идентифицирует личность, кому предназначается сообщение, и автоматически решит, каким способом лучше сообщение до него донести.

Все эти новые коммуникации, как уверяет автор статьи, «будут иметь встроенные защитные устройства, которые надежно предохранят от спама и перехвата, воровства адресных данных и персональной информации». Они позволят обладателям работать более эффективно, креативно, связываться между собой легко и быстро, не завися от устройства, которое в каждый данный момент имеется в руках, или от сети, к которым они подключены.

Как измеряют рентабельность и эффективность охранных программ

Руководители предприятий должны быть заинтересованы в определении эффективности вложений в охрану. Но, наверное, не многие знают, как практически измерять рентабельность, эффективность этого вида деятельности. Обратимся к зарубежному опыту. Американцы, как известно, любят и умеют подсчитывать реальную отдачу от каждого доллара, вложенного в бизнес, включая и косвенные расходы, в том числе на безопасность.

«Метрики могут определить конкретные цифры и контекст осуществления охранной функции, установив прямую зависимость между отсутствием (или наличием) каких-

либо криминальных происшествий и эффективностью программы по охране», отмечает Том Вэйлгам в пространной статье на сайте csoonline.com. Выбор метрик зависит от особенностей организации, профиля деятельности. Инструменты измерения могут быть применимы в одной сфере экономики и бесполезны в другой. Поэтому обратимся к конкретным примерам из практики служб безопасности американских корпораций.

Своим опытом измерения эффективности охранной деятельности делится Фрэнсис Д'Аддарио, глава СБ международной сети кафе Starbucks. Главным приоритетом своей работы он называет безопасность персонала. Здесь основным измерителем служит число разбойных нападений на заведения корпорации. С 1996 года, когда было зафиксировано 46 такого рода инцидентов, их число упало до 11 в 2004 году. Другой путь измерения – сопоставление данных с общенациональной статистикой. На общем фоне безопасность Starbucks также выглядит неплохо (в среднем 45 разбойных нападений на тысячу ресторанов быстрого обслуживания в год – статистические данные цеховых ассоциаций и криминальной полиции).

Д'Аддарио говорит, что снижение количества грабежей обеспечено благодаря проведению специальных обучающих программ с персоналом, призванных помочь служащим предусмотреть и предупредить криминальные инциденты. Также положительную роль играют новые технологии, такие как интерактивные системы оповещения, «умные сейфы» и прочее.

В числе инструментов измерения эффективности безопасности он называет: «отслеживание частоты и результативности бэкграундных проверок персонала, регулярные аудиты системы допусков для служащих, а также контроль за соблюдением правил работы с наличными и имуществом». При этом руководитель СБ подчеркивает, что его методика годится не только для определения эффективности безопасности, но и для проверки профессиональной компетентности и честности служащих. Примером тому служит регулярная выборочная проверка целости грузовых контейнеров (наличие пломб) и соответствия их содержимого заказам и накладным документам. Этим тоже занимается служба безопасности.

Работая в розничной индустрии, Д'Аддарио также анализирует цифры потерь вследствие краж денег и имущества, сравнивает их с аналогичными данными, предоставляемыми (через ассоциации и по иным каналам) другими ведущими в мире компаниями, которые работают в этой же сфере экономики. Полученные аналитические результаты докладываются первым лицам корпорации. Он считает, что, используя разные метрические методы, можно заранее просчитывать то, что называется ROI - Return on Investment (рентабельность инвестиций).

(продолжение в следующем номере журнала)

Новейшие тенденции в сфере охраны американских банков

В конце августа на сайте bankinfosecurity.com размещена статья, посвященная тенденциям в сфере физической охраны американских банков в 2009-2010 годах. Их

всего выделено четыре:

1. Возвращение пуленепробиваемых стекол, защищающих кассы и кассиров в отделениях банков. Еще 10 лет назад отмечалась обратное явление, обусловленное обострением конкуренции, – отказ от некоторых традиционных средств защиты, стремление к упрощению и открытости (в прямом смысле этого слова) в работе с клиентами. Результат оказался двояким: устранение физических барьеров, отделяющих кассиров и банковских операторов от клиентов, что, конечно, не могло не импонировать последним, привело к опасному снижению уровня безопасности на фоне растущей преступности. Теперь полиция ужесточает требования к безопасности в операционных залах финансовых учреждений.

2. Конвергенция физической охраны и Интернет-технологий. Это явление наблюдается в течение последних пяти лет. Конвергенция предназначена для достижения двух задач: повышения уровня безопасности и уменьшения расходов на охрану. Экономический кризис затормозил данный процесс, отмечают эксперты, высказывая в то же время уверенность, что с преодолением кризиса этот процесс будет ускоряться.

3. Возрастающая ставка на аутсорсинг. Не столько технологически, сколько экономически мотивированная тенденция. Оказалось, что проще, дешевле и безопаснее передавать многие функции охраны, в том числе и видеонаблюдение, сторонним профессиональным организациям. Играет свою роль и психологический момент: если что случится, то вину можно возложить на партнера, оставив вне удара собственный имидж, что для финансово-кредитных организаций имеет огромное значение.

4. Усиление внутреннего контроля. Речь идет о регулярных проверках, аудитах, инспекциях всех компонентов безопасности бизнеса. Особого внимания требуют контроль за персоналом и информзащита.

Из истории промышленного шпионажа в современной Америке

Исследование, проведенное американскими экспертами Р. Пауэром и К. Бурджесом, выявили два заблуждения, характерные для управляющих компаниями: недооценка реальной опасности промышленного шпионажа и уверенность, что с защитой коммерческих интересов у них все нормально. В пространной публикации на сайте information-security-resources.com/2009/ они приводят ряд конкретных примеров кражи корпоративных секретов.

Здесь и в последующих номерах нашего журнала мы знакомим читателей с изложением некоторых криминальных историй из практики американских компаний за последние 10 лет.

Lightwave Microsystems

В конце 2002 года частная компания в Калифорнии Lightwave Microsystems объявила о прекращении деятельности в виду финансовых трудностей. Однако неспособность

компании получать прибыль не означает, что она не представляет никакой ценности. У нее есть патенты на собственные изобретения, коммерческие секреты. Позднее она была поглощена другой компанией – Neophotonics, тоже из Калифорнии.

Некий господин Брент Вудворд занимал в Lightwave должность директора по информационным технологиям. Он скопировал хранящиеся на резервных дисках корпоративные секреты и попытался их сбыть прямому конкуренту. Используя псевдоним и созданный для этой цели новый адрес электронной почты, он связался с главным технологом компании JDS-UniPhase, которому и предложил продать скопированную информацию.

Однако, JDS обратилась в Федеральное Бюро Расследований США и согласилось сотрудничать в поимке преступника с поличным. Сотрудники ФБР быстро вычислили, кто скрывался под псевдонимом, и арестовали Вудворда. Ему было предъявлено официальное обвинение, грозившее 10 годами тюрьмы и штрафом $250,000.

Конечно, Бернт Вудворд был просто любителем, действовал исключительно в собственных интересах, школярскими методами. Можно представить, какой урон понесла бы Neophotonics, если бы он вышел на менее разборчивого в вопросах корпоративной этики конкурента.

America Online

В апреле и мае 2003 года программный инженер в компании AOL Джейсон Смазер использовал пароли допуска своего коллеги, чтобы завладеть данными о 30 миллионах клиентах компании. Информация включала электронные адреса, имена и фамилии, телефонные номера, другие важные данные.

Смазер продал список электронных адресов некоему Сену Данэвею за 27 тысяч долларов. Тот использовал эти адреса для рекламы своего коммерческого сайта и затем перепродал профессиональным спамщикам.

Этот случай демонстрирует явную прореху в системе внутреннего контроля AOL. В компании обнаружили утечку информации, но злоумышленнику еще удавалось какое-то время безнаказанно трудиться в обворованной им компании, пока следственные органы не вышли на него. В феврале 2005 года, Смазерс был приговорен к 15 месяцам тюрьмы и штрафу в $84 тысячи.

Компания AOL оценила нанесенный ущерб в $400,000. Но кто подсчитает имиджевые потери компании, которой доверяли десятки миллионов людей?

(продолжение в следующем номере)

Десять недооцененных аспектов охраны предприятия

Продолжаем изложение материала, опубликованного 29 ноября 2006 года под этим названием на сайте www.darkreading.com

7. Обучение персонала

Некоторые наихудшие проблемы с безопасностью возникают из-за элементарной безалаберности сотрудников, например, при работе в онлайновом режиме. Руководство большинства компаний явно недооценивает угрозы с этой стороны.

Проведения раз в год «часа безопасности», когда в течение 30 минут или одного часа в головы работников пытаются уложить все инструкции и рекомендации по безопасности, не достаточно. «Как правило, среднему сотруднику трудно усвоить за один раз все премудрости, связанные с безопасностью, - говорит эксперт по охране предприятия Тодд Фитцжеральд, - необходимы регулярные, более частые тренинги, на которых в доступной форме надо разъяснять и повторять азы безопасности». Учеба должна иметь прикладной характер, с использованием постеров, компьютерных игр, интерактивных технологий, утверждает он.

К сожалению, работа с сотрудниками компании по вопросам безопасности – редкость в наши дни. Руководство компаний рассматривает охрану предприятия с технологической точки зрения, игнорируя ее культурный аспект. Инвестиции в безопасность тратятся на антивирусные программы, детекторы несанкционированных вторжений в компьютерные сети, проверку и тестирование технических средств защиты. При этом недостает понимания, что тренинг персонала - не менее важная составляющая безопасности.

Во многих фирмах сотрудников знакомят с политикой безопасности, с инструкциями по использованию технологий. Но когда политика меняется, а на место старых технологий приходят новые, о переобучении часто забывают.

Конечно, нелегко определить и рассчитать эффективность обучающего процесса. Ключевым моментом здесь является хорошее знание аудитории и понимание, какой уровень обучения необходим. Для разных групп персонала требуются свои учебные программы.

Обучать надо в первую очередь топ-менеджмент. К сожалению, руководители компаний мало что понимают в вопросах безопасности бизнеса. Отсюда – явное недофинансирование и слабая поддержка программ по охране предприятия.

Как остановить воровство в компании

По наблюдению экспертов, уровень воровства на предприятиях и в компаниях в условиях тяжелого финансово-экономического кризиса заметно вырос. «Рецессия не превращает честных людей в преступников», - говорит глава компании SME Management (Анкоридж), Шейла Этеридж, - «но становится предлогом для совершения злоупотреблений теми, кто и ранее об этом помышлял, а тем более совершал правонарушения» (csoonline.com).

В США 70% всех видов преступлений на предприятиях составляют хищения: от фабрикации по сговору с поставщиком фальшивых счетов до воровства ручек, карандашей, бумаги. Но что более всего беспокоит бизнесменов – это как используют увольняемые служащие украденные списки клиентов, маркетинговые данные и другие

коммерческие секреты. По данным Ponemon Institute, 59% работников, уволенных или предупрежденных об увольнении, воруют корпоративные данные, а две трети из них высказывают готовность использовать конфиденциальную информацию на новом месте работы.

Объективная ситуация требует от топ-менеджмента и служб безопасности серьезных усилий по формированию и поддержанию эффективной системы мер своевременного выявления и предупреждения злоупотреблений. Какие меры необходимо предусмотреть? Если не все, то многие ответы на этот вопрос можно найти в публикации “How to Stop Fraud” на сайте csoonline.com (автор публикации Стэси Колет). Вот некоторые из них:

Изучайте характер взаимоотношений между служащими и поставщиками/продавцами – нет ли там семейных, личных связей. Обращайте внимание на немотивированный рост сделок с каким-то одним из поставщиков. Корпоративные финансовые инструкции должны предусматривать разделение функций между теми, кто осуществляет платежи, и кто оформляет входящие средства. Желательно, чтобы платежи осуществлялись специально обученным сотрудником, не являющимся бухгалтером и не имеющим возможность сводить дебит с кредитом.

Неожиданные (внеплановые) аудиты и проверки работы бухгалтерии подтверждают свою эффективность, включая и психологический аспект. Ожидание внезапной проверки удерживает от злоупотреблений.

Даже рутинные финансовые отчеты, если их внимательно изучать, помогут вскрыть нарушения. Например, требуют разъяснений, а то и расследования, необычно возросшие за месяц статьи доходов или расходов.

Огромное значение имеет поддержание на должном уровне физической охраны помещений и периметра здания. Как осуществляется проверка пропусков? Закрываются ли на замок кабинеты, где хранится конфиденциальная документация? Какие меры предпринимаются по контролю за мобильными носителями, такими как ноутбуки. Куда уходит мусор, содержащий бумажные отходы?

В этой связи приходит на память случай с одной крупной американской компанией, которая списывала тонны офисной бумаги в дошкольное учреждение для вторичного использования. И делала это до тех пор, пока один из родителей не нашел на обороте рисунка своего сына номера социального страхования с фамилиями и не заявил об этом в компанию.

Необходимо регулярно, каждую неделю или месяц, проверять допуски сотрудников к внутренней информации, немедленно закрывать допуск увольняемым. Сюда же входит строгий контроль за использованием сотрудниками Интернет-технологий.

Учитывая распространение такой формы работы как «домашний офис», следует время от времени внезапно наведываться к таким работникам домой с проверкой, доступен ли их рабочий компьютер членам семьи, используют ли они надежные шифры, пароли и коды.

И, конечно, нельзя забывать об обучении персонала мерам предосторожности. К примеру, не оставлять около принтера материалы, содержащие финансовую или другую важную информацию, которой может воспользоваться потенциальный

злоумышленник.

регистрация готовые фирмы

Шесть важных рекомендаций тем, кто отвечает за личную охрану

В декабре 2004 года в городе Белфасте вооруженные преступники похитили и взяли в заложники близких родственников двух крупных менеджеров банка Northen Bank, вынудив последних помочь в ограблении банка. Преступление удалось. Заложники вернулись домой.

Эксперты провели исследование, в ходе которого опросили большое число практиков и специалистов по личной охране, в том числе бывших сотрудников секретных служб США, и в итоге сформулировали шесть рекомендаций, имеющих ключевое значение для разработки и осуществления программ по охране персоналий. При этом не важно, идет ли речь о постоянной охране всего руководства компании, или о разовых мероприятиях, связанных, например, с деловой поездкой кого-либо из них. Результаты исследования опубликованы Д.Даффи на сайте csoonline.com.

Рекомендация 1. Ставьте вопросы заранее и часто

Собираетесь вы разработать программу персональной охраны или всего лишь усовершенствовать уже имеющийся план в работе, первым делом надо провести глубокий анализ имеющихся и потенциальных рисков. А именно – идентифицировать людей, играющих критическую роль в организации, просчитать ущерб для компании в случае, если с ними что-то случится, проанализировать риски. Сталкивались ли они в прошлом с угрозами и рисками? Часто ли ездят в небезопасные места? Какого рода преступлениям и или опасным ситуациям более всего подвержены? Как реагируют на окружающую среду – некоторые предпочитают оставаться малозаметными для сторонних лиц, другие, напротив, вовсю себя «пиарят».

Проведя такой предварительный анализ, следует внимательно изучить их частную и публичную жизнь. Здесь охраняемое лицо обязано оказать полную информационную поддержку. Вам надо знать буквально все, в мелочах, о его семье, близких друзьях, о привычках, где и как отдыхает, куда и к кому любит ходить в гости и т.п. Также важно проверить, насколько легко и какими путями посторонние могут получить информацию о персональной жизни охраняемого лица (для этого необходимо, в частности, провести поиск в Интернете, где можно обнаружить подробную информацию о данном персоналии).

На основе всей собранной информации можно приступать к формированию общей картины охранных мер, которые надлежит предпринять. Некоторые нуждаются в минимальной охране. Другие требуют наличия круглосуточной охраны дома и семьи…….
Важно знать сферу бизнеса и учитывать принятые в ней стандарты персональной охраны, используя уже имеющийся опыт.

Конечно, стоимость персональной охраны достаточно велика и требуется убедительная аргументация в пользу ее усиления, а, следовательно, и

дополнительных вложений. При этом надо быть готовым к возможным изменениям, Например, директор компании может получать по электронной почте десятки писем с угрозами, не вызывающих серьезные опасения. Но если в один прекрасный день он находит подобное письмо на пороге своего дома, то это ясный сигнал, требующий принять дополнительные меры охраны.

(продолжение в следующем номере)

Книжное обозрение

Safety and Security Issues in Electric Power Industry
Zdzisław Żurakowski (Institute of Power Systems Automation, Poland)
Springer Berlin / Heidelberg

Книга характеризует различные риски и угрозы для персонала и оборудования, которые необходимо принимать во внимание при проектировании компьютерных систем, используемых в работе электростанций. Впервые для Польши сделан и представлен в книге анализ вопросов защиты и безопасности взаимосвязанных компьютерных систем, установленных на подстанциях высокого напряжения. Эти проблемы связаны в первую очередь с отсутствием в стране стандартов и норм такого проектирования, а также четкой статистики об авариях, остановках и иных инцидентах, происходящих на энергетических объектах. Данные же, которые выдают традиционные контрольные устройства, в большинстве случаев не пригодны для анализа и обобщения. Автор книги дает некоторые рекомендации по улучшению ситуации.

Кризис и информационные утечки: риски растут, меры противодействия ужесточаются

На корпоративном сайте исследовательской компании Proofpoint размещены результаты последнего по времени опроса американских компаний по вопросу об информационных утечках (proofpoint.com, August 10, 2009).

В опросе участвовали компании с численностью персонала более 1 000 человек. Отчет свидетельствует, что на фоне растущих рисков американский бизнес предпринимает драконовские меры противодействия утечкам корпоративной информации. Все больше компаний заявляют о найме людей специально для мониторинга служебной электронной почты (33% против 15% в 2008 г.). Служащих заставляют показывать начальству содержание своей переписки (каждая четвертая американская компания осуществляла выборочную проверку за последние 12 месяцев).

Электронная почта представляет наибольшую опасность. 43% американских компаний

зафиксировали утечки конфиденциальных данных за последний год. Из них каждая третья компания увольняла сотрудников за нарушение инструкции по работе с электронной почтой (31% против 26% в 2008 г.).

Блоговые утечки продолжаются. 18% компаний заявили о случаях утечки данных через блоги. Из них 17% наказали сотрудников, а 9% прибегли к увольнению (в 2008 году 11% и 6% соответственно).

Растут утечки через социальные сети: об этом заявили 17% опрошенных компаний (12% в 2008 г.). За такие проступки 9% компаний прибегли к увольнениям (4% в 2008 г.).

18% американских компаний пострадали от утечек, связанных с увольнением служащих. Около половины опрошенных заявили, что снижение бюджетных расходов и сокращение персонала отдела информационных технологий в условиях кризиса негативно сказалось на информационной безопасности.