Мошенничество с использованием АСУ ТП

На сегодняшний день факт непрерывного роста количества преступлений, связанных с использованием информационных технологий, уже ни у кого не вызывает сомнений. Основной объем киберпреступлений происходит в финансовой сфере, где есть возможность получить незаконный доступ к денежным средствам граждан, организаций и банков. Вместе с тем, в отношении промышленных предприятий и нефинансовых организаций киберпреступления случаются не менее регулярно. Использование мошенниками уязвимостей в промышленных системах автоматизации и наличие возможностей обхода встроенных механизмов защиты информации ставит перед предприятиями принципиально новые задачи в области информационной безопасности.

Согласно обзору экономических преступлений в России за 2016 год, подготовленному компанией PricewaterhouseCoopers, 48% респондентов отметили, что их компании столкнулись с экономическими преступлениями за последние два года, четверть (23%) руководителей предприятий и организаций отметили, что за этот же период их компании пострадали от киберпреступлений. 32% респондентов ощутили рост рисков такого рода мошенничества. При этом часть респондентов не знает о том, что в течение последних двух лет они были взломаны. Также 43% руководителей выразили беспокойство по поводу растущей угрозы киберпреступлений, 52% из них считают ускорение технологических изменений еще одной проблемой. В исследовании 12% респонденов являются руководителями промышленных предприятий, 9% – предприятий ТЭК. Респонденты в России отметили, что ущерб репутации компании и хищение персональных данных являются наиболее разрушительными последствиями этих процессов. Далее идут утрата интеллектуальной собственности и расходы на юридическое обеспечение и принудительное исполнение. На глобальном уровне респонденты отметили сбои в работе/обслуживании, регуляторные риски и непосредственные финансовые потери.

Приведенные выше цифры говорят о том, что значительная часть кибепреступлений носит экономический характер. Преступники используют информационные технологии в целях незаконного обогащения, кражи активов и продукции, фальсификаций бухгалтерской и корпоративной отчетности.

Опыт выполнения проектов ЗАО НИП "Информзащита" в электроэнергетике и нефтегазовой отрасли показывает, что, во-первых, более чем две трети инцидентов в области информационной безопасности происходят по вине или при участии сотрудников предприятий или лиц, имеющих легитимный доступ к информационным системам, и во-вторых, для реализации мошеннических схем все чаще используются автоматизированные системы управления производством и различные системы контроля и учета ресурсов, продукции, энергоносителей.

Исторически вопросы защиты от несанкционированного доступа к программному обеспечению и данным, а также защиты от деструктивного информационного воздействия при создании подобных систем не принимались во внимание. Этими вопросами не занимались ни разработчики, ни проектировщики, ни интеграторы, ни владельцы этих систем. Согласно данным указанного выше обзора, только 26% респондентов подтвердили наличие в их компаниях действующего плана реагирования на инциденты. И это при том, что 47% респондентов указали в ответах, что их компании потеряли до 1 миллиона долларов в результате киберпреступлений, совершенных против них за последние два года, 6% респондентов указали еще более существенный убыток, который они понесли в результате действий мошенников. Стоит отметить, что значительная доля респондентов (23%), компании которых столкнулись с этими проблемами, не могли оценить размер ущерба от них.

Если сравнивать ситуацию с информационной безопасностью в отдельных отраслях, то наибольший объем работ по предотвращению киберпреступлений сегодня ведется в финансовых организациях и банках. Что неудивительно, поскольку степень проникновения информационных технологий в бизнес организаций этой сферы намного превышает по всем показателям ту же электроэнергетику или нефтяную отрасль.

Немаловажным фактором является то, что вопросам защиты АСУ ТП, систем контроля и учета в отечественной промышленности начали уделять внимание совсем недавно, и к реализации реальных мер повышения защищенности таких систем приступили далеко не все предприятия.

Сегодня в России вопросы кибербезопасности АСУ ТП довольно широко обсуждаются профессиональными сообществами, операторами критически важных объектов, производителями компонентов систем автоматизации и средств защиты информации. Основной контекст обсуждений – системы необходимо защищать, потому что взлом и потеря управляемости таких систем несет большие риски в отношении безопасности для граждан, экологии, государственной инфраструктуры. И это действительно так. Но по тем же причинам высоки и риски реализации большого количества мошеннических схем, которые создаются для того, чтобы красть продукцию, подделывать отчетность, незаконно обогащаться и т.д. И вот здесь интенсивность обсуждений участниками рынка значительно меньше. Связь между уровнем защищенности АСУ ТП и рисками использования ее в разного рода мошеннических схемах для большинства участников рынка очевидна, но зачастую вопросами экономической и информационной безопасности в компаниях занимаются разные люди и подразделения. У всех свои должностные обязанности, методики, регламенты, политики. А для того чтобы выявлять схемы мошенничества в таких системах, необходимо объединять подходы и методики проведения аудитов, анализа, инвентаризаций. Пока этого не происходит, злоумышленники будут продолжать пользоваться уязвимостями АСУ ТП в корыстных целях независимо от области их применения или отрасли, в которой они эксплуатируются.

Электроэнергетика

Несовершенство механизмов рыночного регулирования взаимоотношений, а также отсутствие технических средств контроля и выявления отклонений или нарушений в процессе исполнения договорных обязательств между генерирующими, электросетевыми, энергосбытовыми компаниями и потребителями на сегодняшний день дает возможность злоумышленникам использовать различные нелегальные или полулегальные способы получения выгоды при покупке, потреблении и расчетах за поставку электроэнергии, а также в процессе договорных взаимоотношений между участниками рынка электроэнергии.

Среди хорошо известных схем мошенничества, таких как создание фиктивных энергосбытовых компаний, завышение тарифов энергосбытовыми компаниями за счет включения в них инвестиционных расходов, завышения объемов валовой выручки за счет увеличения совокупной мощности оборудования на балансе, довольно широко распространены следующие сценарии:

- незаконные подключения потребителей отдельными сотрудниками электросетевых/энергосбытовых компаний на возмездной основе;
- легальное подключение потребителей с использованием "прокаченных" приборов учета электроэнергии, занижающих показания по реальному объему потребления электроэнергии или отключаемых дистанционно без разрыва соединения в точке подключения;
- внесение изменений в работу автоматизированных информационных систем коммерческого учета электроэнергии (АИИСК КУЭ) отдельными лицами/группами лиц в интересах отдельных потребителей на возмездной основе с целью занижения показаний по объемам реального потребления электроэнергии;
- прямое подключение генераторами потребителей и ведение коммерческого учета по счетчикам, находящимся на балансе у генератора;
- манипуляции с расчетом объемов потребления электроэнергии на собственные нужды при отсутствии автоматизированных систем учета;
- манипуляции с данными при отсутствии автоматизированного переноса данных из систем учета в смежные системы отчетности;
- ручной и непрозрачный расчет технико-экономических показателей на электрогенерирующих предприятиях на основе данных, получаемых из систем коммерческого и технического учета без использования средств связи и передачи данных.

Для того чтобы выявлять большинство из перечисленных выше схем необходимо знать не только состав и уязвимости систем учета, но и понимать суть технологических и производственных процессов, в которых используются такие системы. Необходимо понимать методики расчета большого количества коэффициентов и показателей, описывающих реальное положение дел на предприятии. Без знания отраслевой специфики, а также совместных усилий специалистов в области экономической и информационной безопасности выявлять такие схемы очень сложно.

Нефтедобывающие предприятия

На сегодняшний день уровень автоматизации нефтедобывающих предприятий в среднем выше, чем в электроэнергетике. Вопросы обеспечения экономической и информационной безопасности проработаны довольно глубоко. Тем не менее, при выявлении схем мошенничества все предпринимаемые усилия лежат в основном в области контроля за отчетностью по отгрузкам и контроля за транспортировкой, логистикой, где ведутся систематические сверки показателей по объемам отгрузки, хранения, транспортировки, сро-

кам и полноте оплаты, а также осуществляется постоянный контроль за перемещением транспорта и учет объемов транспортировки в нефтепроводах.

Вместе с тем на предприятиях практически не производится работа по выявлению уязвимостей и способов эксплуатации компонентов и систем коммерческого и технического учета нефти. Опыт проведения аудитов информационной безопасности на месторождениях и предприятиях подготовки нефти показывает, что несмотря на то, что системы учета аттестованы и средства измерений проходят периодические государственные проверки, встроенные механизмы защиты информации и метрологически значимого программного обеспечения в этих системах обходятся довольно легко. Это дает возможность как модифицировать алгоритмы пересчета физических величин или двигать коэффициенты пересчета, так и подменять само метрологически значимое программное обеспечение. Также необходимо учитывать тот факт, что непосредственно на кустовых площадках интеллектуальные измерители объема и качества добываемой суспензии находятся практически в открытом физическом доступе, и многие из них вообще не имеют никаких механизмов защиты от несанкционированного доступа.

Еще один немаловажный аспект – вся корпоративная отчетность по объемам и качеству добываемой суспензии или товарной нефти строится на основании данных, получаемых из систем, находящихся непосредственно на объектах. В случае фальсификации данных в системах учета, являющихся источником для всех остальных корпоративных информационных систем, вся корпоративная отчетность будет оперировать искаженными данными, не отражающими реальные производственные показатели.

Все перечисленные факторы открывают широкие возможности для реализации мошеннических схем, и выявить их только силами специалистов по экономической или информационной безопасности весьма проблематично. Как и в электроэнергетике, требуется знание информационных технологий, экономической и информационной безопасности, особенностей технологических и производственных процессов, математического и метрологического обеспечения систем.

Машиностроение

Металлообрабатывающие и машиностроительные предприятия, особенно имеющие государственные или оборонные заказы, сегодня хорошо оснащены средствами автоматизации производства. В первую очередь это станки с числовым программным управлением. Современные станки объединяют с помощью локальных сетей для того, чтобы иметь возможность централизованно загружать в них управляющие программы, вести мониторинг производственных процессов и диагностику оборудования.

Основной целью злоумышленников на машиностроительных предприятиях являются файлы конструкторской документации из CAD-систем, файлы управляющих траекторий из систем подготовки производства – CAM-систем и непосредственно файлы управляющих программ, получаемые из постпроцессоров или непосредственно со стоек управления станков.

Одна из основных целей хищения указанных видов информации – получение возможности изготовления контрафактной продукции при отсутствии затрат на разработку, то есть со значительно сниженной себестоимостью. Машиностроительные предприятия несут серьезные убытки, когда в поставляемые партии изделий злоумышленники подмешивают контрафактные изделия, в результате чего предприятия в дальнейшем должны выполнять гарантийные обязательства по вышедшему из строя контрафакту.

Зачастую вокруг крупных предприятий создается множество небольших компаний, устанавливающих такие же станки. Получив несанкционированный доступ к управляющим траекториям или программам, они быстро налаживают выпуск "аналогов" продукции предприятия и тем самым приводят в конечном итоге к снижению объемов производства завода. Очень часто учредителями таких компаний являются сотрудники или руководители самого предприятия.

Описанные примеры из электроэнергетики, нефтяной и машиностроительной отраслей, разумеется, не показывают всех аспектов, связанных с мошенничеством. Большое количество преступных схем сегодня реализуется и без использования информационных технологий. Но если с такого рода преступлениями на предприятиях уже давно научились бороться, то использование мошенниками уязвимостей в промышленных системах автоматизации и наличие возможностей обхода встроенных механизмов защиты информации ставит перед предприятиями принципиально новые задачи. Выявлять и пресекать такие схемы сложнее и дороже, необходимо вкладываться в подготовку уникальных специалистов, прорабатывать методики проведения аудитов, проверок, анализа систем.

ЗАО НИП "Информзащита" благодаря большому опыту реализации проектов в области защиты систем, информации, бизнес-процессов, ИТ-инфраструктур оказывает полное содействие промышленным предприятиям и компаниям в решении вопросов по обеспечению защиты производственных систем от мошенничества. Компания имеет ресурсы и компетенции для проведения полного цикла работ в данной области.

Д. А. Даренский,
начальник отдела промышленных систем,
ЗАО НИП "Информзащита"

ГЕОЛОГОРАЗВЕДКА 2016

VOSTOCK CAPITAL

9 НОЯБРЯ, МОСКВА

IT СИСТЕМЫ И ТЕХНОЛОГИИ ДЛЯ ГЕОЛОГОРАЗВЕДКИ:

ВИЗУАЛИЗАЦИЯ, МОДЕЛИРОВАНИЕ, ИНТЕПРЕТАЦИЯ И УПРАВЛЕНИЕ ДАННЫМИ

СРЕДИ VIP-ГОСТЕЙ:

АНДРЕЙ СИМОНОВ

Первый заместитель ген. директора по IT-услугам и проектам, **Башнефть-информ**

АНДРЕЙ ПОПОВ

Начальник управлени информационных технологий и телекоммуникаций, **Газпром геологоразведка**

ВИКТОР ДИКОВ

Директор по развитию и ТО бизнес - сегмента «Геологоразведка и добыча», **Лукойл-информ**

МАКСИМ ШАДУРА

Начальник управления информационных технологий, автоматизации и телекоммуникаций блока разведки и добычи, **Газпром нефть**

ПОДТВЕРЖДЕННЫЕ УЧАСТНИКИ:

ГАЗПРОМ ГЕОЛОГОРАЗВЕДКА · РН-ЭКСПЛОРЕЙШН · БАШНЕФТЬ · НОВАТЭК · БАШНЕФТЬ ИНФОРМ · ГАЗПРОМ ИНФОРМ

ЛУКОЙЛ ПЕРМЬ · НОБЕЛЬ ОЙЛ · РИТЭК · СНГ СУРГУТНЕФТЕГАЗ · ЗАРУБЕЖНЕФТЬ · TATNEFT · РОСНЕФТЕГАЗ

+7 (499) 505 1 505 (Москва), +44 207 394 30 90 (Лондон), events@vostockcapital.com, **www.georazvedkaforum.com**