ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ПРОИЗВОДСТВЕ: ПРОБЛЕМЫ И РЕШЕНИЯ

Стремительное развитие вычислительной техники и информационных технологий породило одну из глобальных задач начала XXI века – обеспечение защиты автоматизированных систем управления производством и создание эффективных систем безопасности производственных активов предприятий. О проблемах информационной безопасности в промышленности и работе своей компании по их решению рассказывает наш гость – Дмитрий Валентинович Рычков, директор Центра промышленной безопасности АО НИП «Информзащита». Вопросы задает главный редактор журнала «Главный инженер. Управление промышленным производством» А.В. Тарасенко.

– Уважаемый Дмитрий Валентинович, как появилась идея создания в структуре «Информзащиты» Центра промышленной безопасности? Какие причины для этого были, какие возможности и какие перспективы?

– Компания «Информзащита» была основана в 1995 году как Научно-инженерное предприятие, и в следующем году мы будем отмечать 25-летие с момента создания. За такой солидный срок мы заработали огромный опыт и безупречную репутацию.

Сегодня «Информзащита» – ведущий российский интегратор в области информационной безопасности (ИБ), который развивает и поддерживает широкий спектр услуг по внедрению, экспертизе, поддержке и сервисному обслуживанию комплексных систем обеспечения и управления ИБ.

В середине 2000-х годов от заказчиков стали поступать запросы на проведение обследований производственных и технологических сегментов корпоративных сетей промышленных предприятий, что потребовало выделение группы специалистов компании в Отдел промышленных систем для адаптации имеющихся методик и компетенций к специфике работы промышленного производства. В 2017 году в АО НИП «Информзащита» был создан Центр промышленной безопасности (ЦПБ), в состав которого вошли специалисты с опытом в области информационной и промышлен-

На сегодняшний день в Группу компаний «Информзащита» входит пять компаний:

- *НИП «Информзащита»;*
- *«Информзащита-Сервис»;*
- *«Код безопасности»;*
- *«Национальный аттестационный центр»;*
- *Учебный центр «Информзащита».*

Компании группы являются сертифицированными партнерами крупнейших мировых поставщиков решений по безопасности, среди которых IBM Internet Security Systems (IBM ISS), Лаборатория Касперского, Positive Technologies, Check Point Software Technologies Ltd., HP ArcSight, Cisco Systems, Stonesoft, Fortinet, Imperva, InfoWatch, «КриптоПро», Websense и многие другие.

Рычков Д.В.,
директор Центра промышленной безопасности АО НИП «Информзащита»

ной безопасности. Целью его создания стала реализация сложных проектов по защите автоматизированных систем управления технологическими процессами и SCADA-систем, систем управления производством (MES), систем управления жизненным циклом сложных изделий (PLM).

Таким образом, создание ЦПБ стало ответом на потребности инновационной части промышленности в разработке и внедрении систем безопасности дорогостоящих производственных активов. Перспективная задача Центра – создавать комплексные системы безопасности для решения широкого перечня проблем, стоящих перед управленцами, производственниками и службами безопасности предприятий, которые могут затрагивать, кроме собственно информационной безопасности, и физическую, и экономическую, и другие специфические виды безопасности, присущие той или иной области производственной деятельности.

– Какие основные проблемы информационной безопасности (и «опасности») Вы можете назвать: в целом и для российских промышленных предприятий, в частности?

– Проблем информационной безопасности много, а у промышленных предприятий тем более. И поверьте, я не преувеличиваю.

Начнем с того, что информационная безопасность уже по определению защищается, а значит, нападающие всегда на шаг впереди, как минимум в своих преступных намерениях. Без принятия этого базового понимания нельзя правильно оценивать перечень проблем и подходов к их решению.

Поэтому если исключить финансовую отрасль, где у банка крадут «живые» деньги, оборонную промышленность, государственные учреждения, а также силовые структуры, где защищаются интересы государства и его основ, то все остальные должны еще доказать себе и своим акционерам необходимость информационной безопасности в качестве превентивной меры.

Это, собственно, и есть Проблема №1 – понять сам факт необходимости мероприятий по ИБ для организации.

Но даже те, кто осознает потребность в ИБ, сразу же сталкиваются с тем, что это затратное мероприятие. Безусловно, предприятия разные, и доходы/расходы у них отличаются. Для кого-то миллион рублей – это погрешность бюджета операционной деятельности, а для кого-то - безумная трата, превышающая годовой бюджет развития производственных мощностей.

Таким образом, Проблема №2 – это определение размеров и выделение финансирования на ИБ. Причем по нашему опыту именно в такой последовательности: «определили – надо, но выделим деньги, наверное, когда закончится мировой кризис».

Области деятельности типового предприятия в направлениях работы Центра промышленной безопасности АО НИП «Информзащита»

И здесь снова руководитель рассуждает с точки зрения, в первую очередь, простых правил человеческой логики – стоимость защиты не должна быть больше стоимости возможных потерь от реализованной угрозы. Если у меня валовый объем всех производственный участков суммарно не более 100 млн руб. в год, то зачем мне превентивные меры ИБ даже на половину этой суммы, если может что-то случиться, а может и не случиться.

Ни для кого не секрет, что деньги выделяют собственники и работающие на них финансисты. Поэтому задача заключается в том, чтобы должным образом представить проект ИБ и его последующие результаты. Просто рассказать страшилки мало. Ответ руководителя будет прост и лаконичен: «Ну, до этого-то у нас подобного не случалось». И возразить трудно. Но и без страшилок нельзя – учиться лучше на чужих ошибках (чуть позже я обязательно приведу примеры).

Так вот, речь о том, каков он, тот правильный ракурс описания влияния угроз ИБ на бизнес, который убе-

дит лиц, принимающих решение, что у ИБ должно быть достойное финансирование, и это не пустые траты, не выброшенные на ветер деньги акционеров. В каждом случае, безусловно, этот вопрос решается индивидуально. Хотя на деле это бесконечное многообразие особенностей различных отраслей тоже поддается классификации для определения соответствующих эффективных ИБ-решений.

Итак, понимание первыми лицами производственной компании важности мероприятий ИБ трудно переоценить. И такое понимание эффективно только в том случае, если позицию не просто принимают, а разделяют руководители всех направлений предприятия и, собственно, персона, отвечающая в компании за технологии и производство.

Называться этот человек может по-разному: технический директор, заместитель директора по производству, вице-президент производственного блока и т.п. По сути, для своей компании он все равно остается самым главным инженером.

Соответственно, наипервейшая задача Центра промышленной безопасности – помочь производственникам и асушникам разобраться, что для них важно, что не важно, что для них нужно, а без чего можно обойтись. И главное, и это особенность работы в области защиты АСУ ТП, а что вообще не надо делать, дабы не поставить под угрозу выпуск продукции. Для нас как исполнителя по проекту ИБ наше искреннее, но коммерческое желание – не просто получить деньги, а заработать их, да еще потом гордиться выполненным проектом. Или, как принято говорить, – получить референтного заказчика.

При этом, с одной стороны, к нам как к известной на рынке компании обращается очень много заказчиков со своими запросами, но, с другой стороны, рынок услуг ИБ, как и любой другой, – очень конкурентный, и надо обязательно быть чем-то лучше, чтобы работали именно с нами.

Ну и Проблема №3, вытекающая из предыдущей, – это проблема окупаемости ИБ-проектов.

И тут есть разные подходы к расчету окупаемости: минимум - два, максимум – бесконечность. Первый из двух подходов – научный. В мире люди разговаривают на разных языках, но работают на похожих производствах и, соответственно, решают схожие проблемы. Есть понятие IT Science – то есть ИТ-наука, в России нам широко известны пока только такие понятия, как область информационных технологий/информационной безопасности или, в новом видении – цифровая трансформация. Поэтому, очевидно, и научные методы обоснования окупаемости ИБ-проектов (а они реализуются ИТ-средствами – программным обеспечением и программно-аппаратными комплексами) у нас с расшифровками от иностранных сокращений: NPV, RR, ROI, ALE и проч. Но это нисколько не мешает использовать их для экономически рассчитываемого обоснования окупаемости проекта ИБ. Кстати, в одной интересной зарубежной методологической работе о кибербезопасности в области энергетики, вышедшей в этом году, целый раздел посвящен именно стоимости (ее математическому/экономическому обоснованию) управления ИБ – Cost of Cybersecurity Management. Про понятия информационной безопасности и кибербезопасности можно поговорить отдельно.

Второй подход – экспертный. В классической математике он назывался бы методом экспертных оценок, хотя на сегодняшний день есть и мно-

го более популярных в консалтинге признанных интерпретаций.

И первый, и второй подход наш Центр промышленной безопасности использует в совершенно конкретной повседневной проектной деятельности. Если перечислить основные темы, которыми мы занимаемся, то это:

- проведение категорирования объектов критической информационной инфраструктуры (КИИ) в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и другими законодательными и отраслевыми требованиями (и не только КИИ);
- разработка проектов защиты объектов КИИ и/или ЗОКИИ (значимых объектов КИИ) и других проектов, связанных с вопросами защиты информации и кибербезопасности на предприятии;
- исполнение проектов.

Именно при выполнении таких работ появляются конкретные оценки значимости мероприятий ИБ для предприятия и соответствующие оценки стоимости решений ИБ.

Назвав три общие основные проблемы, можно продолжать и дальше, но в ответ на Ваш вопрос, хотелось бы теперь упомянуть проблемы промышленного сектора в РФ. И разговор пойдет только о производственной деятельности, промышленных предприятиях и безопасности.

Итак, коротко:

Информационные процессы на усредненном промышленном предприятии не являются определяющими, на первом месте всегда безотказная работа производственного оборудования. Заниматься ИБ можно только так, чтобы не навредить.

Отсюда, Проблема №1 – «ИБ на производстве надо поднимать, но крайне осторожно…» – проблема ограничения возможного контроля угроз ИБ в промышленной сети предприятия в силу особенностей эксплуатации технологического оборудования.

Иностранные разработчики производственных линий (механизмов, агрегатов, прокатных станов, станков) превалируют почти во всех типах современного производства. Оборудование стоит дорого и имеет сложную и закрытую цифровую «начинку». Находится, по возможности, на гарантийной и сервисной поддержке производителя.

Отсюда, Проблема №2 – «Чтобы заниматься ИБ на производстве, надо понимать и в производстве!» – проблема планирования и реализации мероприятий ИБ на производстве, задействования квалифицированных кадров.

У нас в «Информзащите» этот вопрос решен и организационно, и технически. Такие работы выполняются специалистами, имеющими компетенции одновременно в сетевых технологиях, информационных системах, системах АСУ ТП, а также понимающих особенности подходов крупных производителей технологий к вопросам безопасности.

И, наконец, Проблема №3 (ограничим бесконечность списка) – невозможность рассмотрения мероприятий ИБ без учета мероприятий собственно промышленной безопасности (транспортной, энергетической и др., в зависимости от отрасли).

Последний упомянутый пункт может еще кому-то показаться спорным. Но, если вспомнить, что объекты КИИ определяются именно по степени возможного ущерба для окружающей среды и социума (кто сомневается, может перечитать упомянутый выше Федеральный закон № 187-ФЗ и приказы Федеральной службы по техническому и экспортному контролю, ФСТЭК России), то, без учета влияния угроз ИБ на поведение систем промышлен-

ной безопасности средств противоаварийной защиты (ПАЗ), систем взрывопожаробезопасности, ну и, конечно, человеческого фактора – т.е., в том числе и систем охраны труда (ОТ), наверное, всерьез рассматривать эффективность мероприятий ИБ в сегодняшнем цифровом мире смартфонов и повсеместного Интернета уже неправильно.

Поэтому проект ИБ в промышленном сегменте – это на самом деле наведение порядка, чтобы «не взрывалось и не ломалось». Хотя экспертное мнение нашего Центра, что не надо под зонтик ИБ тянуть вообще все. Как минимум, уже заявляемые связки с ТОиР и корпоративными бизнес-процессами на даже очень продвинутых промышленных предприятиях РФ, на рубеже сегодняшнего 2019 года, - это перебор. Хотя новые проблемы уже засвечиваются на горизонте.

Например, из-за осложнения с 2014 года общеполитической ситуации некоторые руководители ИБ крупных предприятий очень правильно озаботились вопросом контроля процессов гарантийной и сервисной поддержки основного технологического оборудования. Мало того, что собственно первые линии поддержки находятся в неизвестных географических точках, но и само обращение (заведенный «тикет») может обрабатываться и Бразилии, Индии или на Гонолулу (страны названы из реальных кейсов).

Ну и тогда несколько страшилок, конечно, без адресов и фамилий:

- одна крупная российская компания была очень «взбудоражена» (мягко сказано), когда сотрудники ИБ-департамента обнаружили и доложили руководству, что сеансы удаленного доступа к системе управления технологическим оборудованием основного производства ведутся не из сети производителя в Германии (как должно было быть по сервисному контракту), а с адреса IP-сети интернет-кафе в дальнем областном центре России. До выезда группы захвата не дошло, но мероприятия ИБ были существенно ужесточены, а виновные наказаны;
- не единичный, но в данном случае конкретный пример: полная остановка на несколько дней систем с группой компьютеров, подцепивших вирус-шифровальщик. Производственные процессы были переведены на ручное управление, по агрегатам назначили внеплановое профилактическое обслуживание. С проблемами после безуспешных попыток борьбы справились только полными переустановками систем, что потребовало, в том числе, и привлечения иностранных специалистов производителя (соответствующие счеты были выставлены). Виновные были наказаны. Ущерб производству является коммерческой тайной предприятия;
- на пограничных сетевых устройствах российского завода с интересной продукцией постоянно присутствует активность с IP-адресов из региона Юго-Восточной Азии. Ситуация не может быть как-то разрешена полностью, так как места источников меняются. Адекватным ответом ИБ-службы на данный момент является только укрепление периметров и сокращение возможных поверхностей атак;
- из официально опубликованного, это инцидент в крупной энергетической компании: отключение без разрешения технологического оборудования принудительно через средства удаленного доступа;
- ну и, наконец, несколько блэкаутов в 2019 году, в том числе Венесуэла – просто отключили свет.

Перечни хакерских атак опубликованы в аналитических материалах специализированных российских и зарубежных компаний. Мы сейчас об этом говорить не будем – да, хакеров ста-

ло еще больше. Но интереснее другое – появился новый тренд: хакеры в 2018-2019 годах обратили свое внимание на промышленные компании. Почему? Очень просто: «Стратегия синего океана» и развитие технологий Интернета вещей. Стоимость взлома меньше и безопаснее, чем для банка. И если дойти до подмены транзакций, то можно затеряться в субподрядных юридических лицах (особенно, если это строительство крупных промышленных объектов) и направить часть денежных средств в свой адрес. При этом «ломать» надо не управляющую компанию, которая, как правило, защищена и технологически, и организационно, а какую-нибудь IP-камеру на заводе или стройплощадке, что повышает вероятность не быть пойманным до 99%. Вот такие новые метаморфозы киберпреступлений.

– Какие продукты «Информзащита» может предложить производственникам, промышленным предприятиям? Предприятия холдинга выпускают какое-либо свое оборудование?

– На сайте нашей компании написано «"Информзащита" – системный интегратор». Это означает, что продукты мы предлагаем не какие-то строго определенные, а те, которые решат поставленную задачу. Но так как ЦПБ – это все-таки часть компании, но специализированная, то мы действительно отличаемся в технологиях и зачастую в вендорах.

Если коллеги из смежных подразделений работают по оборудованию Cisco, Palo Alto, «Континент», ViPNet и похожих брендов – то наши специалисты на объектах чаще встречаются с другими названиями: Siemens, Moxa, Belden, Schneider, Honeywell, Yokogawa, Hirschmann и т.д.

На одних и тех же вендорах, таких как Лаборатория Касперского, «Позитив Технолоджис», Infowatch наш Центр работает с продуктами своей направленности: KICS, ISIM, ARMA.

Наши внедрения проходят и там, где развитые инфраструктуры с продуктами компании Microsoft, и на специализированных производствах, где работают продукты на базе «Альт Линукс», «Астра Линукс» и других Линукс-клонов.

Там есть место и PAM-системам управления привилегированными учетными записями и продвинутым системам контроля целостности ПО. В наш же контур входят и защита уровня MES- и PLM-систем.

Если говорить собственно про условно прикладной уровень, то в отличие от наших коллег из просто ИБ, которые защищают финансовые, бухгалтерские, управленческие системы, файловые хранилища и т. п., мы больше работаем со SCADA-системами, инженерными станциями. Хотя по иерархии продуктов ИБ потребителями информации от нас являются те же SIEM, SOC, GRC.

Кратко излагая основы нашей концепции защиты предприятия, перечислю только общие темы:

- идентификация и аутентификация;
- управление доступом;
- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности и доступности;
- защита технических средств и систем;
- защита информационных (автоматизированных) систем;
- реагирование на инциденты ИБ и обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Если говорить о темах, которые наш Центр предлагает дополнительно к обсуждению своим заказчикам, то это:

• информационная безопасность в процессах повышения коэффициентов безостановочной работы;

• информационная безопасность в процессах промышленной безопасности и охраны труда;

• информационная безопасность в процессах сервисной поддержки основного технологического оборудования.

Отвечая на вторую часть вопроса, – да, предприятия группы компаний выпускают собственное аппаратное оборудование и программное обеспечение к ним. Это в первую очередь очень известные на российском рынке бренды: «Континент», SecretNet, «Соболь», vGate. Не так часто, но наш центр пересекается в технологических областях и с этим оборудованием.

– SOC (Security Operations Center) для промышленного предприятия – насколько и когда он нужен, каковы его задачи, насколько затратен? Какой персонал должен обеспечивать его работу?

– Он очень нужен, но он и очень затратен. Предприятие в принципе должно заниматься выпуском своей продукции, предоставлением своих услуг. Несвойственные функции правильнее отдавать на аутсорсинг. Если еще раз вспомнить Федеральный закон № 187-ФЗ, то там четко дано понимание, что все объекты ЗОКИИ в итоге будут подключены технологически или организационно к ГосОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак).

Вопрос про персонал правильный. Персонал должен быть высококвалифицированным на специализированных темах мониторинга событий, работа круглосуточная, и это опять же не очень соотносится с основными целями производства по выпуску продукции.

Поэтому, по возможности – на аутсорсинг.

– Каким Вы видите «цифровое промышленное предприятие» в России?

– Цифровое предприятие – это автоматизированное и роботизированное предприятие, где большинство процессов выполняется без участия человека. Там мало сотрудников и много компьютеризированного оборудования. Таких предприятий уже и сейчас много, точнее - на почти каждом успешном предприятии есть хотя бы один цех или участок, похожий на вышеописанную картинку.

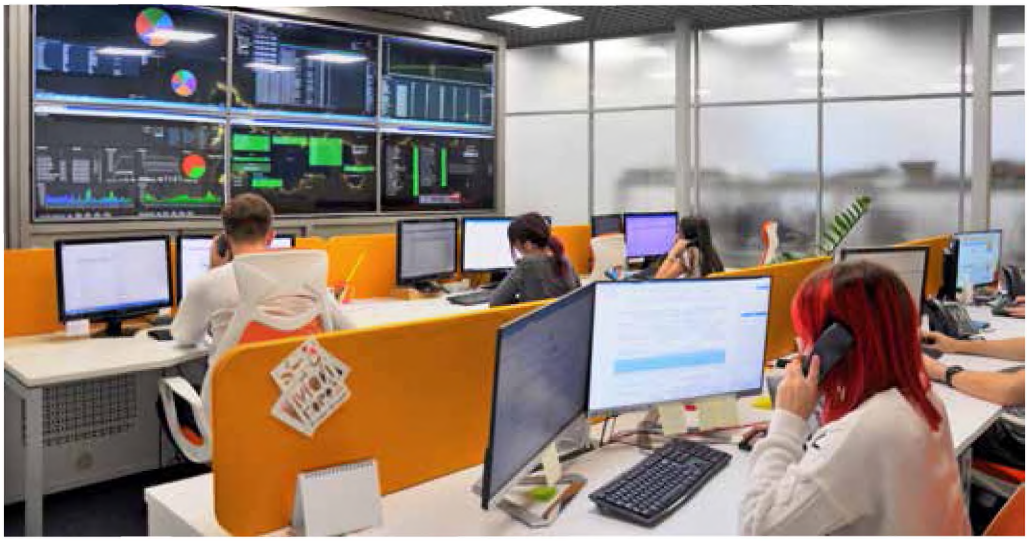
Для примера, найдите людей на территории завода на современном автомобилестроительном или пивоваренном предприятии. Нет никого – только в зоне разгрузки/погрузки. Потому что, либо специалисты находятся вблизи оборудования – контролируют процесс (в сборочном цеху, конечно, могут что-то и прикручивать), либо находятся в операторских за стеклом и перед пультами.

Маленький нюанс: там стоят закупленные производственные линии иностранного производства. И дальше все те проблемы ИБ, о которых мы уже говорили ранее.

С другой стороны, в России есть предприятия, где ручной труд очень мало автоматизирован, – литейное производство одного регионального завода приходит на память, механосборочный цех одного столичного завода – там белых халатов нет и, наверное, не скоро они там могут появиться.

Но и те, и другие предприятия имеют свои угрозы информационной безопасности. Только эти угрозы сильно отличаются и по масштабам возможного ущерба, и по компенсирующим мероприятиям.

– Существуют ли сегодня в России промышленные предприятия, близкие к реализации концепции



Круглосуточный Центр мониторинга инцидентов безопасности АО НИП «Информзащита» (SOC)

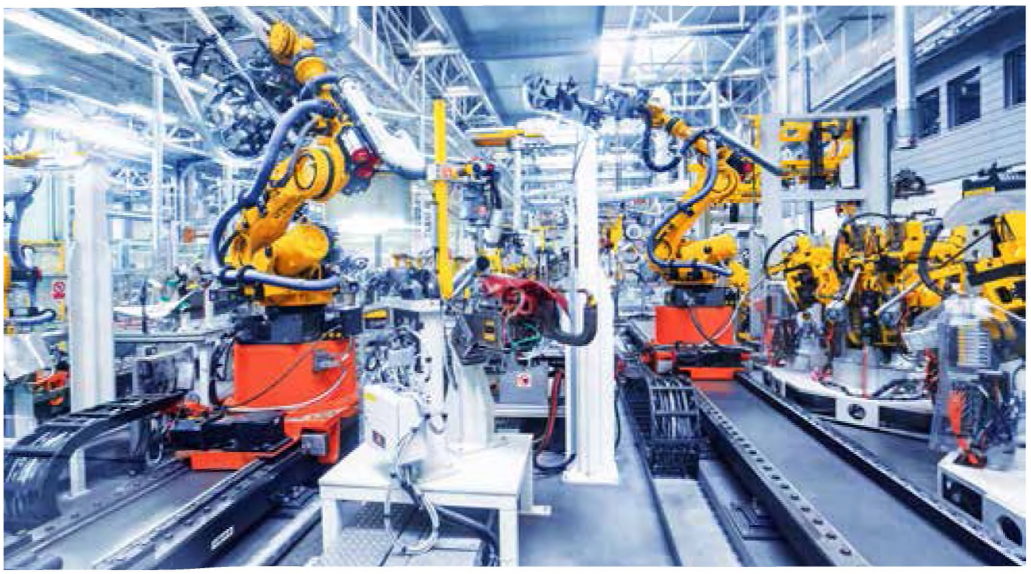
«цифрового предприятия»? А за рубежом?

– Существуют. За рубежом тоже. И зависит все не от места расположения этого предприятия, а от того, какой уровень автоматизации был заложен при его создании или модернизации.

– Выпускники каких ВУЗов работают на предприятиях холдинга, какие специальности востребованы больше всего?

– Очень разных ВУЗов, хотя сейчас много выпускников именно факультетов, связанных с информационной безопасностью.

Озвучу свое частное мнение. Многие студенты факультетов информационной безопасности считают, что они не должны быть экспертами в информационных технологиях. Практика показывает, что это пагубное заблуждение. Не нужен в информационной безопасности специалист, особенно молодой специалист, который не разбирается в том, в чем разбирается специалист ИТ, АСУ или хакер. Да, конечно, нельзя знать всего,



Сборочный цех современного роботизированного предприятия

но иметь знания определенного уровня практически во всех компьютерных областях, а со временем и опыт в своей специализации/области производства, и, конечно же, «страсть к секьюрити» и экспертные знания в области кибербезопасности специалист ИБ в наше время просто обязан!

В действительности это очень сложно, поэтому мы отчасти воспитываем кадры сами. Есть стажерская подготовка, есть студенческие практики, есть студенческий резерв.

– Каких крупнейших заказчиков Вашей продукции из промышленного сектора экономики (из разных отраслей, если можно) Вы можете назвать?

– В настоящее время специалисты Центра промышленной безопасности выполняют проекты на предприятиях металлургической, химической, нефтегазовой и других отраслей промышленности. Из известных российских компаний это: горно-металлургическая компания «Металлоинвест», международная сталелитейная компания «НЛМК», Магнитогорский металлургический комбинат, Объединенная компания «РУСАЛ», АО «Саянскхимпласт», ПАО «Уралкалий», АО «РОСПАН ИНТЕРНЕШНЛ». Другие наши заказчики не менее заметны на рынке РФ. В том числе, и заказчики из сектора оборонной промышленности.

Благодарю Вас, Дмитрий Валентинович, за столь подробные ответы на вопросы, интересующие руководителей российских промышленных производств в наше суровое с точки зрения обеспечения информационной безопасности время. От имени всех наших подписчиков и читателей разрешите пожелать НИП «Информзащита» дальнейших успехов, а Вам лично – доброго здоровья, хорошего настроения, новых профессиональных и творческих достижений!

Иллюстрации предоставлены АО НИП «Информзащита»