Выступление председателя Правления МОО «Национальный комитет общественного контроля М.Р.Юсупова на Форуме 09.02.2017 года

Негативное влияние коррупционных факторов на обеспечение безопасности критически важных объектов.

В настоящее время ни одна организация не застрахована от различного вида криминальный опасностей и угроз, тем более от коррупционных проявлений, которые способны не только нанести существенный урон деятельности этой организации, но создать реальную опасность для людей и в целом всей страны особенно на критически важных объектах, где степень опасности с учетом особенностей в несколько раз выше.

Критически важные объекты — это объекты, оказывающие существенное влияние на национальную безопасность Российской Федерации, прекращение или нарушение функционирования которого приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны, либо для жизнедеятельности населения, проживающего на соответствующей территории, на длительный период времени и со значительными негативными последствиями.

К сожалению, всем известно, что за последние десятилетие во всех сферах жизнедеятельности государства и общества глубоко проникли и установились коррупционные отношения, не обошли они и деятельность КВО.

В реальности от коррупции страдают почти все и государственные, общественные и бизнес структуры в том, числе объекты повышенной опасности. И опасность данного факта в том, что все это охватывается во временном и большом территориальном пространстве, что трудно контролировать и предотвращать.

Проблема обеспечения безопасности критически важных объектов национальных инфраструктур не является новой. Практически эта проблема всегда на острие у государства. Ей уделяется большое внимание, поскольку любое развитие КВО связано с усложнением всех процессов, обеспечивающих ее целенаправленную деятельность.

В настоящее время обеспечение безопасности КВО является одной из первоочередных задач государства, поскольку любая авария на КВО может привести к широкомасштабной катастрофе не только для данной территории, но и для многих других стран. Пример – Чернобыльская катастрофа.

Сегодня повышение опасности, связанной с нарушением работы различных КВО определяется рядом факторов, отражающих существующую реальность.

Первый фактор – это тенденция к постоянному усложнению всех процессов деятельности и исполнительного оборудования во всех сферах деятельности. Тенденция проявляется в постоянной и все ускоряющейся смене – 10–15 лет - технологических укладов в промышленности и управлении, в стремлении к повышению качества жизни людей и, соответственно, расширением и усложнением системы обеспечения, давно уже имеющей характер промышленного производства.

Второй фактор - наличие и развитие комплекса потенциальных воздействий – угроз, реализация которых приводит к нарушениям нормального режима функционирования объекта. Источниками таких угроз могут являться как внешние враждебные действия, так и непреднамеренные или преднамеренные действия персонала, ошибки или недоработки при проектировании и эксплуатации процесса, различного рода нарушения регламентных правил выполнения процесса, природные явления и т.д. Очевидно, что такого рода угроз может быть достаточно большое множество и ряды их пополняются постоянно, а возможный нанесенный ущерб – увеличивается. В качестве примера можно рассматривать появление и бурное развитие угроз информационного воздействия (кибератак) на ход выполняемых процессов с целью нарушения их нормального выполнения.

Третий фактор – широкомасштабное применение для управления всеми процессами различного рода автоматизированных систем, современных средств и систем связи, включая Интернет, что значительно повышает эффективность процессов. Однако, при этом возникает новая область реализации угроз - уязвимости автоматизированных систем и систем связи, воздействие на которые приводит к большому ущербу, а в условиях недостаточного знания всего состава кибератак – к значительному повышению опасности возникновения критической ситуации на КВО.

Четвертый фактор – это коррупционный фактор, когда при проведении тендеров на различные формы содержания, охраны объектов, техническое обслуживание и закупку нового оборудования КВО за место изношенного и многое другое чаще всего сопровождается **коррупционными откатами**, в результате которых не хватает средств на закупку надлежащего оборудования, либо обеспечения надлежащей охраны и решения многих особо-важных задач по обеспечению надлежащей работы КВО. В результате искусственно, коррупцией создается реальная угроза техногенных аварий и ЧП.

Безусловно сложилось так, что системы обеспечения безопасности критических объектов (СОБ) разрабатывались под определенные комплексы угроз, т.е. от террористических, информационных, природных угроз и т.д.

Но в настоящее время когда коррупционные факторы и проявления охватили почти все сферы деятельности государства и общества возникла новая проблема и серьезная угроза в области деятельности критически важных объектов, которая как скрытая и завуалированная, оказывает негативное

влияние на всех стадиях и технического обслуживания и морально духовного состояния специалистов, работающих в указанной особо-важной сфере.

И поэтому наравне решения всех проблем очень важно уделить внимание предупредительным антикоррупционным мерам в деятельности КВО. Необходимо установить антикоррупционный общественный контроль при проведении конкурсов и тендеров, проводимых в области КВО, проведение профилактических и предупредительных мер, антикоррупционного просвещения работников КВО, подбору персонала, совершенствования законодательной базы и многое другое.

В соответствии с принятой идеологией определялись соответствующие комплексы потенциальных угроз по данному направлению, точки процесса и объекта, где эти угрозы могут быть реализованы (уязвимости объекта), составлялся свод правил (требований), определяющих набор разного рода мероприятий (организационных, технических, идеологических, экономических и др.), выполнение которых определяло защиту выявленных уязвимостей от заданных угроз. Априори предполагалось, что выполнение всех регламентирующих требований обеспечивает безопасность процесса и объекта в целом. Создаваемая система ориентировалась на контроль, фиксацию состояния критических точек и выполнение набора требований по защите известных уязвимостей от известных потенциальных угроз именно данного направления и представляла собой конгломерат слабо взаимодействующих отдельных подсистем по каждому типу угроз.

Критерием обеспечения безопасности являлось выполнение требований, вне зависимости от того, каким образом это определяется. Необходимо отметить, что не выполнение требования определяет появление риска возникновения критической, аварийной ситуации, величина риска является оценкой обеспечения безопасности процесса или объекта. К сожалению, в принятой идеологии оценка риска в большинстве оценивается не расчетами, а экспертами.

Исходя из-за краткости времени для обсуждения вышеуказанных проблем, хочу предложить усиление внимания и контроля со стороны государства и надзорных органов власти по всем изложенным факторам и особенно необходимости проведения антикоррупционных мер на всех стадиях деятельности КВО, необходимости общественного контроля и профилактических и предупредительных комплексных мер.

Список использованной литературы:

1. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (16 июля 2012г.)

2. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Указ Президента Российской Федерации от 15 января 2013г. №31с

3. Кононов А.А., Стиславский А.Б., Цыгичко В.Н. Управление рисками нарушения транспортной безопасности. –М.; АС-Траст, 2008. -210 с.

4. Нечаев Д.Ю., Черешкин Д.С. Управление комплексной безопасностью КВО на основе оценки рисков возникновения чрезвычайных ситуаций // Перспективы развития технических наук. Выпуск II. Сборник научных трудов по итогам международной научно-практической конференции (6 июля 2015г.). – Челябинск, 2015, - с.18-28

5. Цыгичко В.Н. Оценка эффективности систем обеспечения информационной безопасности объектов национальной инфраструктуры// Современные проблемы и задачи обеспечения информационной безопасности/ Труды Всероссийской научно-практической конференции «СИБ-2014». –М.; МФЮА, 2014. - 80-89 с.

6. Цыгичко В.Н., Стиславский А.Б Формальная постановка задачи обеспечения безопасности транспортного комплекса // Управление рисками и безопасностью: Труды Института системного анализа Российской академии наук. Т. 41 - М.: ЛЕНАНД, 2009, стр. 26-42

7. Цыгичко В.Н., Черешкин Д.С. Безопасность критически важных объектов транспортного комплекса. Lambert Academic Publishing, Saarbrucken, 2014.- 217 с.

8. Черешкин Д.С. Аппаратно-программный комплекс обеспечения антитеррористической безопасности (на примере транспортного комплекса) //Труды СПИИРАН. СПБ, ООО «Политехника-сервис», 2010. т.1

9. Черешкин Д.С., Цыгичко В.Н., Кононов А.А. Задачи управления без опасностью региональной информационной инфраструктуры // Науч.-техн. информ. - Сер.1. - 2003. - №