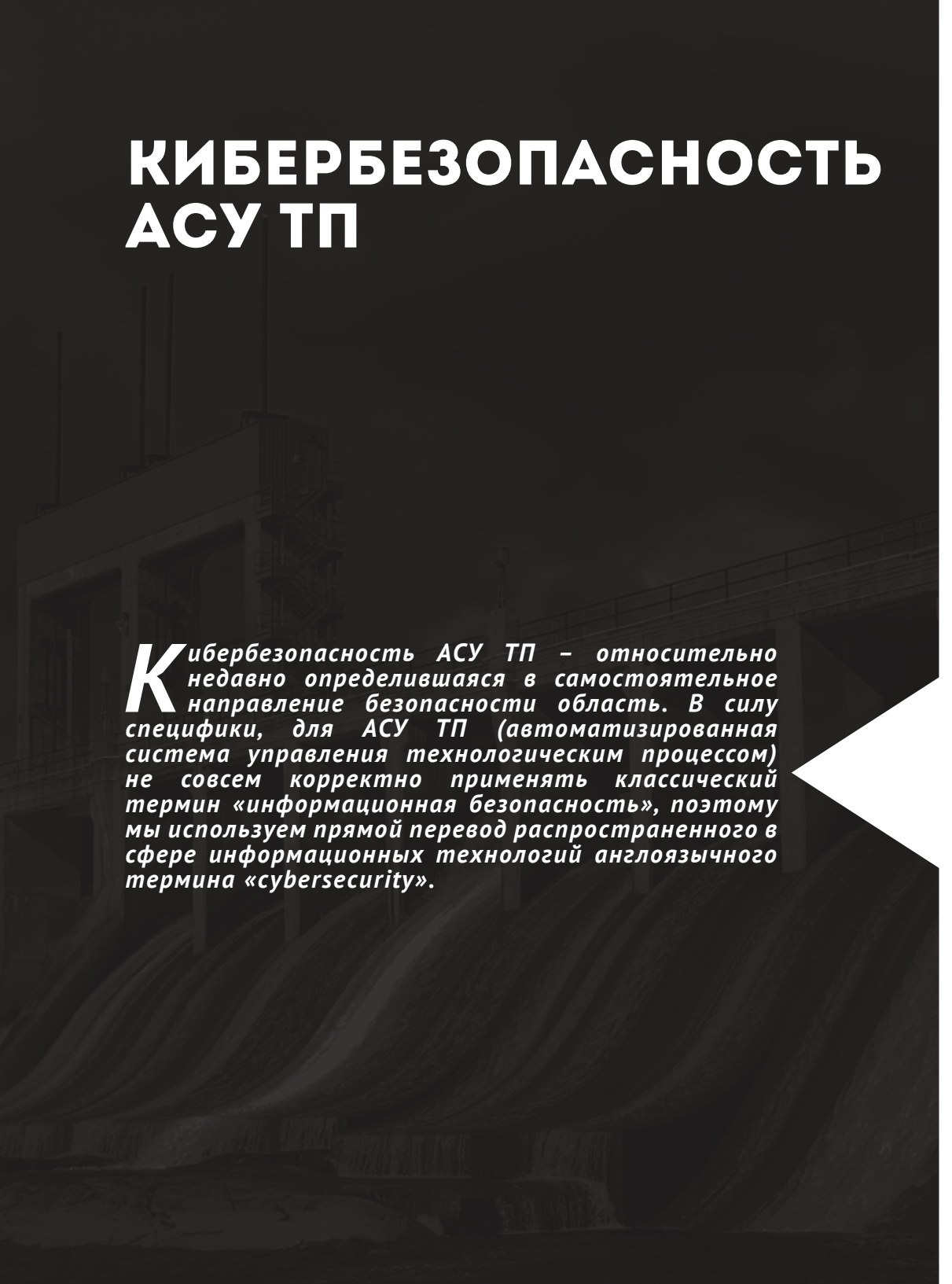
ДиалогНаука

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ АСУ ТП

КИБЕРБЕЗОПАСНОСТЬ АСУ ТП



Кибербезопасность АСУ ТП – относительно недавно определившаяся в самостоятельное направление безопасности область. В силу специфики, для АСУ ТП (автоматизированная система управления технологическим процессом) не совсем корректно применять классический термин «информационная безопасность», поэтому мы используем прямой перевод распространенного в сфере информационных технологий англоязычного термина «cybersecurity».

АО «ДиалогНаука» предлагает услуги в области обеспечения кибербезопасности АСУ ТП, систем телемеханики и информационной инфраструктуры промышленных объектов в целом.

Мы обеспечиваем повышение уровня защищенности АСУ ТП и промышленных объектов в целом от киберугроз, а также соответствие руководящим и нормативным документам РФ. При этом мы опираемся на международные стандарты и лучшие мировые практики в области кибербезопасности АСУ ТП:

• РД ФСТЭК по обеспечению безопасности Ключевых систем информационной инфраструктуры (КСИИ).

• Приказ ФСТЭК № 31 от 14 марта 2014 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

• Семейство стандартов IEC 62443, пришедшее на смену семейству ISA99, подробно и детально описывающее требования и рекомендации по моделированию угроз, анализу рисков, мерам кибербезопасности, внедряемых на протяжении всего жизненного цикла систем АСУ ТП.

• SP-800-82 Guide to ICS security, содержащий подробные рекомендации по построению защищенных АСУ ТП начиная с уровня сетевой архитектуры до уровня конфигураций контроллеров и SCADA-систем, а также описывающий организацию процессного обеспечения ИБ.

… и другие специфичные для отрасли нормативные документы и стандарты.

ЭТАПЫ РАБОТ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ АСУ ТП

01 ПРЕДПРОЕКТНОЕ ОБСЛЕДОВАНИЕ

На основе собранной информации проводится:

• анализ автоматизированных технологических и бизнес-процессов, определение критичных узлов и информационных потоков;
• определение и анализ уязвимостей;
• анализ рисков кибербезопасности;
• моделирование угроз;
• моделирование нарушителя;
• моделирование объекта защиты и сегментирование АСУ ТП на зоны безопасности;
• определение текущего и целевого уровня безопасности;
• разработка требований/рекомендаций по обеспечению мер кибербезопасности.

02 ПРОЕКТИРОВАНИЕ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ

На основании проведенной при обследовании оценки рисков и построенной модели угроз, разрабатывается комплекс организационно-технических мер кибербезопасности. Меры кибербезопасности выбираются с учетом определенного порогового риска и с «запасом», учитывающим постоянное снижение их эффективности с течением времени (появление новых уязвимостей и методов атак, устаревание технологий защиты и т.п.). Полученный комплекс мер становится основой для разработки требований или технического задания на систему кибербезопасности. При проектировании мы рассматриваем не только периметр АСУ ТП, но все уровни вплоть до контролеров. Мы сотрудничаем с различными производителями систем АСУ ТП и при разработке мер защиты осуществляем макетирование и стендовые испытания технических решений, проверяя их эффективность и надежность.

03 ВНЕДРЕНИЕ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ АСУ ТП

Для внедрения технических и программных средств кибербезопасности в обязательном порядке разрабатывается комплекс мер, обеспечивающий минимальные нарушения доступности ресурсов и минимальные прерывания (или полное их отсутствие) в технологических процессах Заказчика.

Внедрение системы кибербезопасности АСУ ТП не ограничивается непосредственно «установкой и настройкой СЗИ». Мы оказываем помощь в выстраивании необходимых процессов кибербезопасности на объекте защиты, осуществляем разработку регламентов, процедур и процессов всего жизненного цикла кибербезопасности (в том числе процессов выявления и реагирования на инциденты, управления всеми компонентами и функциями системы, планирования действий по ИБ и т.д.)

04 СОПРОВОЖДЕНИЕ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ АСУ ТП

В сопровождение системы обеспечения кибербезопасности АСУ ТП могут входить:

- консультации по базовой установке, штатной работе и обновлению средств защиты;
- проведение повторного аудита и оценки рисков, пересмотра политик кибербезопасности и организационно-распорядительной документации;
- проведение работ по масштабированию или модернизации систем обеспечения кибербезопасности АСУ ТП;
- проведение работ по адаптации системы обеспечения кибербезопасности АСУ ТП и документации под изменения в нормативных документах.

05 ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ

Развитие современных технологий компьютерных атак, выявление новых уязвимостей в программном обеспечении, появление новых средств и методов обеспечения кибербезопасности, постоянно изменяющееся поле угроз и рисков приводят к необходимости постоянного мониторинга рисков и переоценки эффективности реализованных мер кибербезопасности.

АО «ДиалогНаука» предлагает своим клиентам услуги, направленные на поддержание адекватного уровня кибербезопасности:

- Анализ уязвимостей, в т.ч. с использованием инструментальных средств защиты (в сегментах, где это реализуемо без риска нарушения технологического процесса);
- Пересмотр моделей угроз и результатов анализа рисков объекта защиты;
- Оценка эффективности действующих мер (систем) обеспечения кибербезопасности;
- Разработка и внесение изменений или модернизация системы обеспечения кибербезопасности, в том числе изменений в процессах обеспечения жизненного цикла кибербезопасности.

НАШ ОПЫТ

Компания «ДиалогНаука» работает в области защиты АСУ ТП на протяжении нескольких лет.
В нашем портфеле есть следующие крупные проекты:

Аудит корпоративных и технологических сегментов электросетевой компании

В рамках аудита технологических сегментов было проведено в т.ч. инструментальное сканирование уязвимостей выделенных технологических сегментов, а также анализ конфигураций телекоммуникационного, серверного и ПЛК-оборудования.

В результате аудита был выявлен целый ряд уязвимостей, составляющих риски кибербезопасности объекта, как на сетевом, так и на серверном уровнях технологических сегментов систем АСУ ТП, ТМ. В рамках проекта были разработаны модели угроз для систем диспетчерского и оперативно-технологического управления, телемеханики, АИИСКУЭ. По результатам аудита были разработаны рекомендации по реализации мер обеспечения кибербезопасности технологических сегментов.

Проектирование подсистемы обеспечения информационной безопасности автоматизированной системы управления нефтебазовым хозяйством

В рамках работ был проведен аудит АСУ НБХ, моделирование угроз и анализ соответствия руководящим и нормативным документам.

На основе результатов сотрудники АО «ДиалогНаука» выполнили комплекс работ по техническому проектированию подсистемы обеспечения ИБ.

Создание системы обеспечения информационной безопасности комплекса автоматизированных систем технологического управления электросетевой компании

АО «ДиалогНаука» осуществляет полный комплекс работ по созданию системы обеспечения информационной безопасности автоматизированной системы технологического управления (АСТУ) одной из крупнейших в Москве электросетевых компании.

В рамках работ осуществлено предпроектное обследование комплекса систем АСУ ТП и ТМ, входящих в состав АСТУ, включающей в себя более 2000 объектов.

В ходе проектирования системы специалистами АО «ДиалогНаука» был разработан ряд уникальных технических решений, реализующих механизмы информационной безопасности непосредственно на уровне оборудования АСУ ТП.

Создание систем защиты от киберугроз технологических сегментов (АСУ ТП) гидроэлектростанций

В настоящее время специалистами АО «ДиалогНаука» ведутся работы по предпроектному обследованию автоматизированных систем управления технологическими процессами объектов (5 ГЭС, расположенных в различных регионах РФ), моделирование угроз безопасности, проектированию системы защиты от киберугроз.

После завершения проектных стадий будет осуществлена поставка средств защиты, пусконаладочные работы и введение системы в эксплуатацию.

ПРОДУКТОВАЯ ЛИНЕЙКА

АО «ДиалогНаука» один из первых системных интеграторов, реализующих в своих проектах функции централизованной аутентификации, обеспечения целостности, криптографической защиты информации (в т.ч. с поддержкой алгоритмов шифрования ГОСТ) и ЭЦП на уровне ПЛК АСУ ТП. Это один из возможных подходов к реализации мер кибербезопасности. Также в рамках работ по защите АСУ ТП АО «ДиалогНаука» применяет как высокоуровневые средства защиты информации, хорошо зарекомендовавшие в корпоративном сегменте, так и средства защиты и технические решения, разработанные специально для защиты АСУ ТП.

PHOENIX CONTACT

Компания “PhoenixContact”, одна из мировых лидеров в разработке и производстве электротехнических компонентов и систем промышленной автоматизации, разработала линейку промышленных межсетевых экранов в защищенном от внешних воздействий исполнений PhoenixContacnt mGuard. Решения mGuard способны обеспечить функции межсетевого экранирования, резервирование каналов связи (с использованием встраиваемого 3G модуля), VPN, контроль целостности (с использованием дополнительного программного модуля), контроль положения и точного времени (с использованием встраиваемого GPS приемника) и др.

SYMANITRON

Российский производитель оборудования связи для промышленных систем передачи данных выпускает ряд промышленных коммутаторов/маршрутизаторов с функциями межсетевого экрана, обеспечивающих:

- SCADA брандмауэр с поддержкой анализа протоколов Modbus, IEC101/104, DNP3.0
- Функции VPN-агента с поддержкой SSH-туннелей, L2 и L3 режимов, IKE, AES и 3DES шифрования;
- Поддержку стандарта IEEE 802.1x;
- Наличие встроенных сотовых модемов 2G/3G.

«Лаборатория Касперского» разрабатывает специализированные решения, предназначенные непосредственно для защиты промышленных объектов и АСУ ТП. Среди продуктовой линейки Лаборатории есть в т.ч.:

- антивирусные решения, разработанные специально для критических объектов и систем реального времени, для которых недопустимо негативное влияние на производительность и надежность систем;
- комплексные решения по защите конечных устройств, в т.ч. способные обеспечить контроль целостности программных компонент ПЛК;
- решения по созданию системы мониторинга и анализа, способной контролировать легитимность трафика между SCADA-системой и автоматическим оборудованием, осуществляющим управление технологическими процессами.

Решения компании Palo Alto networks позволяют осуществлять сегментирование, межсетевое экранирование, потоковую антивирусную защиту, обнаружение и предотвращение вторжений (сетевых атак) в сетях АСУ ТП. Решения класса NGFW, помимо «традиционных» функций, поддерживают сигнатурный анализ специфичных сетевых атак для протоколов Modbus, DNP3, CIP Ethernet/IP, IEC 60870-5-104, OPC и многих других. Широкий функционал и большой выбор аппаратных платформ позволит подобрать решение практически для любых задач в области защиты АСУ ТП.

Высококвалифицированные консультанты компании АО «ДиалогНаука» подберут наиболее удобную форму предоставления услуги и оптимальный состав работ, исходя из индивидуальных особенностей Вашей организации, а также из соображений экономической эффективности выполняемых работ.

Решения на базе HP ArcSight являются отличной основой для создания SIEM-систем, обеспечивающих сбор и анализ корреляции событий ИБ с устройств различных уровней АСУ ТП (в т.ч. с устройств уровня ПЛК), выявление и сигнализацию об инцидентах информационной безопасности.

ИнфоТеКС – один из ведущих производителей программных и программно-аппаратных VPN-решений и средств криптографической защиты информации также разрабатывает средства межсетевого экранирования и средства криптографической защиты информации (с поддержкой алгоритмов шифрования ГОСТ и сертификацией ФСБ) для обеспечения защиты АСУ ТП и промышленных объектов.

Более 20 лет «ДиалогНаука» является одной из ведущих российских компаний, специализирующихся в области информационной безопасности.

«ДиалогНаука» оказывает услуги в области системной интеграции, консалтинга и внедрения комплексных решений по защите информации. Компания является членом АЗИ, АДЭ, НП «АБИСС», АП КИТ, является сертифицированным партнёром BSI Management Systems CIS и имеет свидетельство об аккредитации в области персональных данных от Роскомнадзора. Система менеджмента качества сертифицирована на соответствие требованиям ISO 9001:2008. Система менеджмента ИБ сертифицирована в соответствии с ГОСТ ИСО 27001.

Компания имеет аккредитации QSA и ASV, позволяющие проводить аудит и ASV сканирования уязвимостей в соответствии с требованиями стандарта PCI DSS.

Свою деятельность «ДиалогНаука» осуществляет на основании лицензий ФСТЭК, ФСБ и Министерства обороны РФ.

контактная информация:

117105, Москва, ул. Нагатинская, 1
Тел: +7(495) 980 67 76
Email: info@dialognauka.ru
Website: www.dialognauka.ru

Тел: +7 (495) 980-67-76 // Email: info@dialognauka.ru // Web: www.dialognauka.ru