КОД ИБ | ЕКАТЕРИНБУРГ 2023

НЕЯВНАЯ УГРОЗА: как наличие поставщиков услуг снижает защищенность предприятий от компьютерных атак

Христолюбова Анна Анатольевна

НПП “Гамма”

ФГУП «НПП «ГАММА»
ЕКАТЕРИНБУРГСКИЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР
26 октября 2023 г.

Источники угроз безопасности

Оказание услуг подрядными организациями (аутсорсинг)

Поверка средств для измерений	**Техническое обслуживание и эксплуатация сетей газопотребления и газового оборудования**	**Аутсорсинг информационных ресурсов**	**Поставка оборудования для автоматизации критических процессов**	**Техническое обслуживание оборудования, пусконаладочные шефмонтажные работы, гарантийное и постгарантийное обслуживание**

Каковы последствия?

Последствия инцидента	Угрозы
Н.14 Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса.	УБИ.3 Угроза несанкционированной модификации (искажения) УБИ.4 Угроза несанкционированной подмены УБИ.5 Угроза удаления информационных ресурсов УБИ.6 Угроза отказа в обслуживании УБИ.7 Угроза ненадлежащего (нецелевого) использования УБИ.8 Угроза нарушения функционирования (работоспособности) УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника
Н.16 Необходимость дополнительных (незапланированных) затрат на восстановление деятельности	УБИ.3 Угроза несанкционированной модификации (искажения) УБИ.4 Угроза несанкционированной подмены УБИ.5 Угроза удаления информационных ресурсов УБИ.6 Угроза отказа в обслуживании УБИ.8 Угроза нарушения функционирования (работоспособности) УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника
Н.24 Неспособность выполнения договорных обязательств	УБИ.3 Угроза несанкционированной модификации (искажения) УБИ.5 Угроза удаления информационных ресурсов УБИ.6 Угроза отказа в обслуживании УБИ.7 Угроза ненадлежащего (нецелевого) использования УБИ.8 Угроза нарушения функционирования (работоспособности)

Поверка средств для измерений

ГОСТ РВ 0015-002-2020

П. 7.1.5.11 Технические средства для мониторинга и измерения должны быть защищены от несанкционированного доступа, способного повлиять на достоверность результатов измерений (испытаний)

МИ 3286-2010
Рекомендация. Проверка защиты программного обеспечения и определение ее уровня при испытаниях средств измерений в целях утверждения типа

Технические средства для мониторинга:

Технические и программные средства для информационных технологий, непосредственно применяемые для мониторинга продукции и процессов.

Средства контроля

Индикаторы

Технические средства для измерения:

Средства измерений

Эталоны единиц величин

Стандартные образцы

Испытательное оборудование и технические системы (комплексы) полигонов, испытательных организаций (испытательное оборудование).

Техническое обслуживание и эксплуатация сетей газопотребления и газового оборудования

Категория источника угроз ИБ	Описание источника угроз ИБ
Внутренние антропогенные	Инженерный персонал
	Вспомогательный персонал, обеспечивающий эксплуатацию
	Работник, ответственный за обеспечение ИБ
	Работники обслуживающей организации
	Руководители структурных подразделений (главный инженер)
Внешние антропогенные	Работники аварийно-диспетчерской службы обслуживающей организации
	Уволенные работники Общества
	Злоумышленники
Внутренние техногенные	Аппаратные компоненты сети газопотребления, подверженные компьютерным атакам
	Программные компоненты сети газопотребления, подверженные компьютерным атакам
	Инженерно-технические компоненты сети газопотребления, подверженные компьютерным атакам
Стихийные (непреднамеренные)	Стихийные источник угроз (наводнения, затопления, грозы и т.д.)

•См.:

- ГОСТ 34741-2021 «Системы газораспределительные. Требования к эксплуатации сетей газораспределения природного газа»
- Приказ Минэнерго России от 06 ноября 2018 г. № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования»

Аутсорсинг информационных ресурсов

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
Статья 13. Информационные системы
Статья 16. Защита информации

СП.4.11 Внедрение вредоносного ПО через компрометацию инфраструктуры подрядчика, среды сборки разработчика (подрядчика) и (или) службы технической поддержки

ГОСТ Р ИСО/МЭК 27002—2012
п.6.2 Аспекты взаимодействия со сторонними организациями

Цель: Обеспечивать безопасность информации и средств обработки информации организации при доступе, обработке, передаче и менеджменте, осуществляемом сторонними организациями.

Если имеется потребность в работе со сторонними организациями – проводить оценку риска для определения последствий для безопасности и требований к мерам и средствам контроля и управления. Меры и средства контроля и управления следует согласовывать и определять в договоре (контракте) со сторонней организацией

Техническое обслуживание оборудования, пусконаладочные шефмонтажные работы, гарантийное и постгарантийное обслуживание

ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

Приложение А, А.14.2.7
Разработка с использованием аутсорсинга .
«Организация должна осуществлять надзор и мониторинг разработки систем, выполняемой подрядчиками »

A.11.2.4
Техническое обслуживание оборудования

«Должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной доступности и целостности»

См.: *NIST Cybersecurity Framework (PR.MA-1, PR.DS-8, PR.MA-2)*

Техническое обслуживание и ремонт оборудования должны проводиться под контролем, заранее согласованными способами и инструментом

После проведения ремонта и технического обслуживания программная и техническая части должны проверяться на предмет целостности соответствующими инструментами

Техническое обслуживание и ремонт оборудования, в том числе удаленным способом, должно быть согласовано со службой ИБ, и осуществляться с использованием способов, которые не допускают несанкционированный доступ

Поставка оборудования для автоматизации критических процессов

Установление в договорах (контрактах) требований к осуществлению удаленного технического обслуживания и диагностики только посредством объектов информатизации, в отношении которых реализован тот же уровень защиты (в том числе защиты информации), что и в отношении обслуживаемых объектов информатизации

Аудит (последующий контроль) и анализ операций, осуществляемых в рамках удаленного технического обслуживания и диагностики

Разработка и внедрение **процедуры предоставления поставщику услуг доступа к защищаемой информации и инфраструктуре организации**
(в рамках действующей системы менеджмента ИБ)

Фиксирование обязанностей и разделение зоны ответственности поставщика услуг и организации в обеспечении ИБ при проведении работ (оказании услуг)

Установление требований в договоре (контракте) к гарантиям поставщика услуг (в том числе финансовым) в случае наступления риска нарушения ИБ

Отраслевой центр компетенций по ИБ в промышленности Минпромторга России

https: //ock.gammaural.ru

t.me/ockgammaural