Екатеринбургский НТЦ ФГУП «НПП «Гамма»

Защита информации на оборудовании с ЧПУ - уязвимости, угрозы и риски

Директор Екатеринбургского НТЦ ФГУП «НПП «Гамма»,
Худеньких Александр Сергеевич,
начальник отдела сертификации
Екатеринбургского НТЦ ФГУП «НПП «Гамма»,
Бондин Андрей Рудольфович

Екатеринбургский НТЦ ФГУП «НПП «Гамма»

Приказом Минпромторга России от 02.04.2009 г. № 210дсп на ФГУП «НПП «Гамма» возложены функции головной организации по информационной безопасности

ГАРАНТ Информационно-правовой портал

Главная страница | Документы системы ГАРАНТ | Искать другие документы

Указ Президента РФ от 29 мая 2008 г. N 861 "О внесении изменения в перечень стратегических предприятий и стратегических акционерных обществ, утвержденный Указом Президента Российской Федерации от 4 августа 2004 г. N 1009"

Скачать

ТЕКСТ ДОКУМЕНТА | АННОТАЦИЯ | ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

ФГУП "Научно-производственное предприятие "Гамма" (г. Москва) включено в перечень стратегических предприятий. Продукция (работы, услуги) предприятий, включенных в указанный перечень, имеет стратегическое значение для обеспечения обороноспособности и безопасности государства, защиты нравственности, здоровья, прав и законных интересов граждан РФ. Ликвидация и реорганизация стратегических федеральных государственных унитарных предприятий осуществляются Правительством РФ на основании решения Президента РФ.

ФГУП "НПП "Гамма" является головной организацией по информационной безопасности в Федеральном агентстве по промышленности. Среди основных направлений деятельности предприятия - оказание услуг по противодействию иностранным техническим разведкам и технической защите информации; разработка, проектирование и производство средств защиты информации, средств контроля защищенности информации; специальные экспертизы и сертификационные испытания.

1 Уязвимости и угрозы

2 Внешние риски со стороны регуляторов

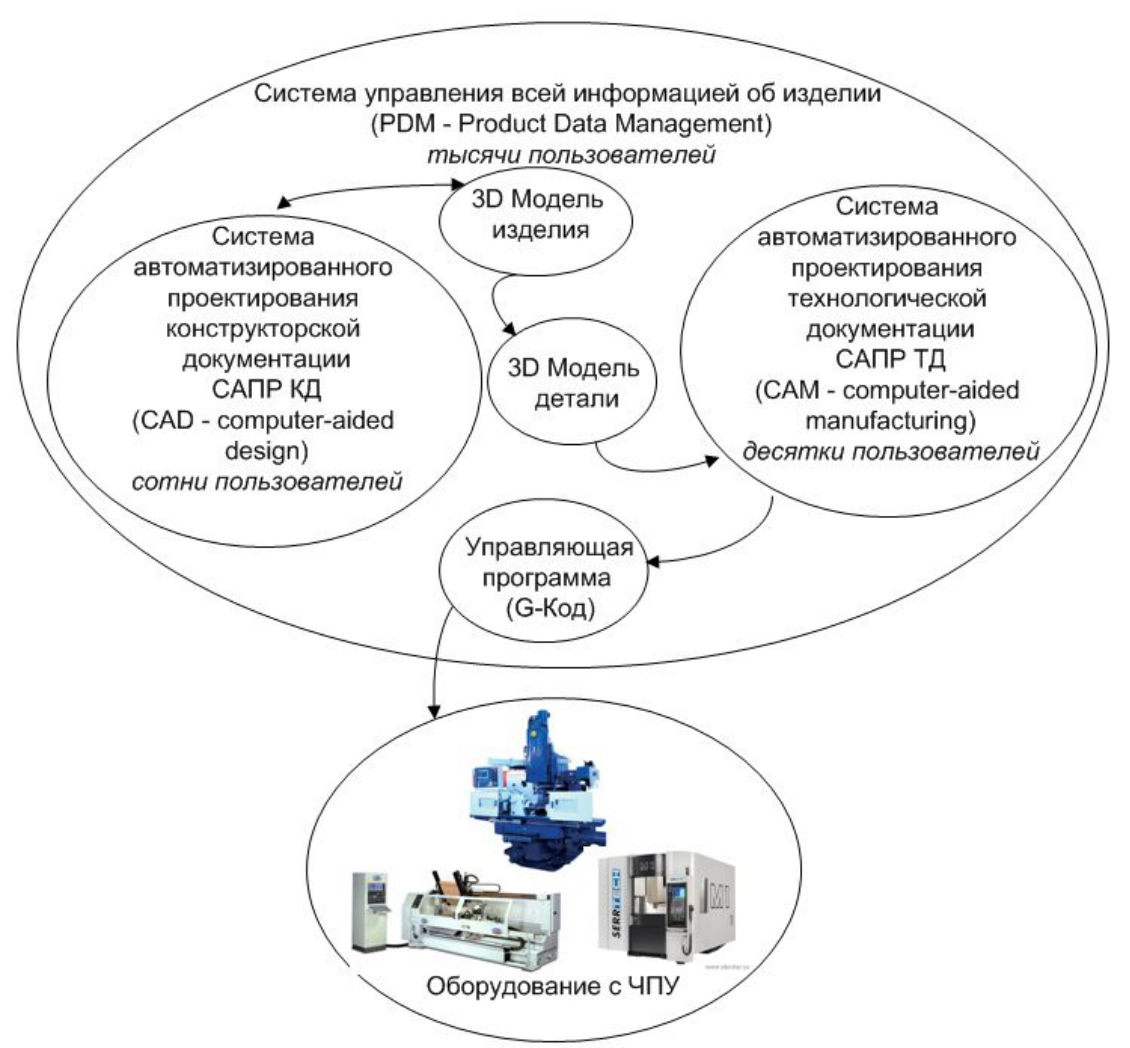
3 Риски нарушения непрерывности бизнеса

4 Два подхода к защите информации и общие рекомендации

1 Уязвимости и угрозы

Структуру информационных систем промышленного предприятия

Оборудование с ЧПУ в системе сквозного параллельно проектирования



Вынужденное применение иностранного оборудования и заимствованного программного обеспечения

Уровень исходной защищенности – обычно нет подключения к внешним сетям связи (Интернет)

Угроза – активация аппаратных и программных закладок

Источник угрозы – представители спецслужб иностранных государств

Отсутствие ЗИП

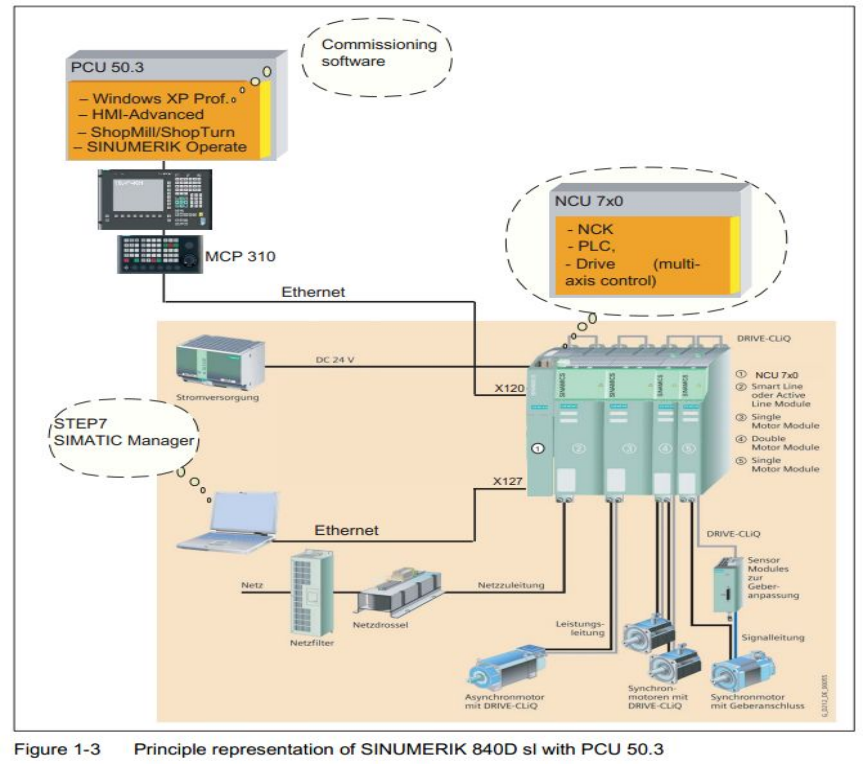


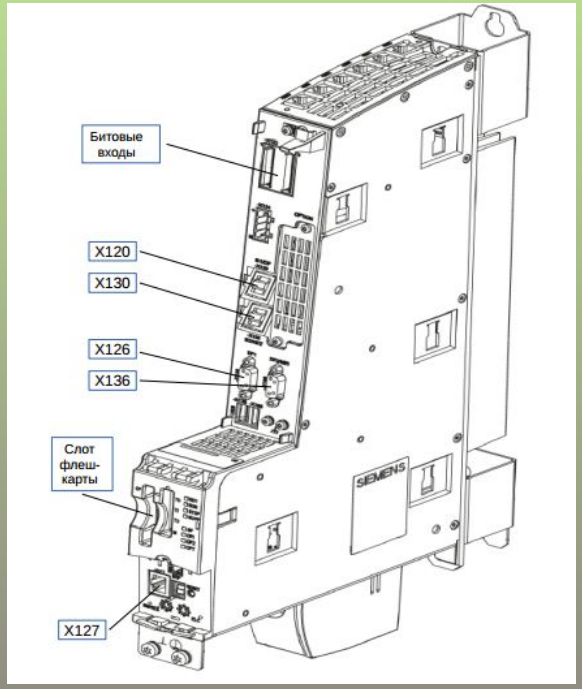
Figure 1-3 Principle representation of SINUMERIK 840D sl with PCU 50.3

Система ЧПУ SINUMERIK 840D sl – архитектура типа «звезда»

Угроза – аппаратный сбой

Источник угрозы – техногенные факторы

Открытые порты

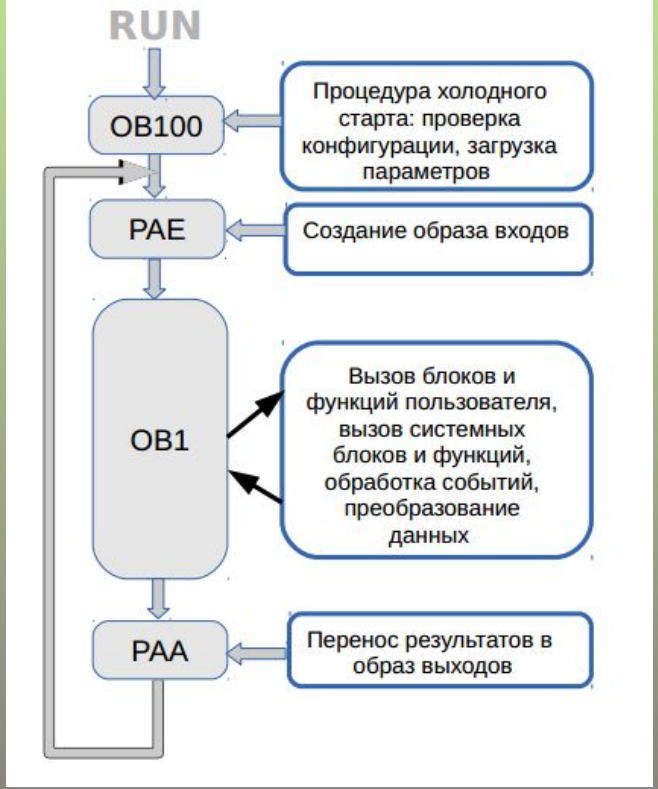


Модуль NCU 7x0.3

Угроза – компьютерная атака

Источник угрозы – внутренний нарушитель (представители спецслужб иностранных государств)

Системы реального времени



Программный цикл PLC в рабочем режиме RUN
Угроза – компьютерная атака
Источник угрозы – внутренний нарушитель (представители спецслужб иностранных государств)

2 Внешние риски со стороны регуляторов

Обязательность соблюдения конфиденциальности информации

Федеральный закон Российской Федерации
«Об информации, информационных технологиях и о защите информации»
от 27 июля 2006 г. № 149-ФЗ.

Статья 9. Ограничение доступа к информации
*2. **Обязательным** является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами*
3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Положение по защите информации при использовании оборудования с числовым программным управлением, предназначенного для обработки информации ограниченного доступа, содержащей сведения, составляющие государственную тайну, утвержденное приказом ФСТЭК России от 25 февраля 2009 г. № 07.

По информации, циркулирующей на оборудовании с ЧПУ, возможно восстановить сведения о нормах расхода сырья и материалов, сведения производственного и технологического характера.
Федеральный закон Российской Федерации от 29 июля 2004 года № 98-ФЗ
«О коммерческой тайне»

«Положение по защите информации при использовании оборудования с числовым программным управлением, предназначенного для обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну», утвержденное приказом ФСТЭК России от 29 мая 2009 г. № 191

Обязательность защиты информации

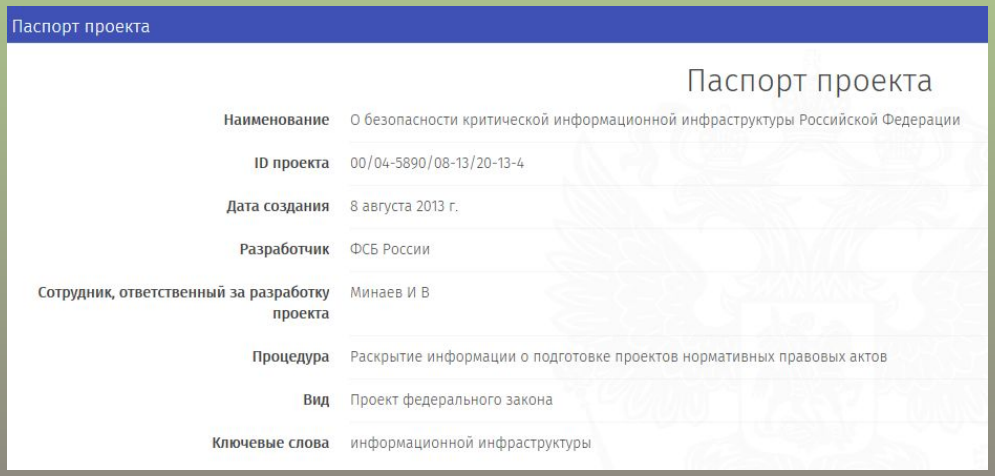
Федеральный закон Российской Федерации
«Об информации, информационных технологиях и о защите информации»
от 27 июля 2006 г. № 149-ФЗ

Статья 6. Обладатель информации
*4. Обладатель информации при осуществлении своих прав **обязан**:*
2) принимать меры по защите информации;

Статья 16. Защита информации
*4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, **обязаны** обеспечить:*
1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
…
4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
…
6) постоянный контроль за обеспечением уровня защищенности информации.

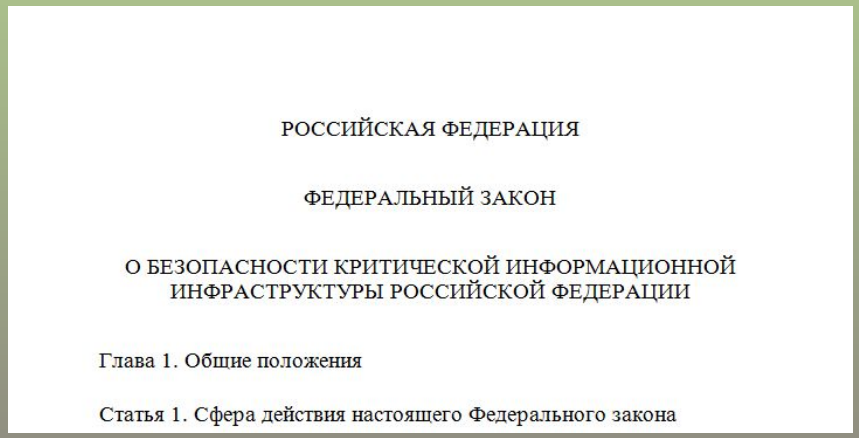
Проект Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации“

(подготовлен ФСБ России, выложен сайте на сайте regulation.gov.ru, http://regulation.gov.ru/projects#npa=5971 доработанный текст проекта акта 00_04-5890_08-13_20-13-4)


Паспорт проекта

Паспорт проекта

Наименование	О безопасности критической информационной инфраструктуры Российской Федерации
ID проекта	00/04-5890/08-13/20-13-4
Дата создания	8 августа 2013 г.
Разработчик	ФСБ России
Сотрудник, ответственный за разработку проекта	Минаев И В
Процедура	Раскрытие информации о подготовке проектов нормативных правовых актов
Вид	Проект федерального закона
Ключевые слова	информационной инфраструктуры


РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

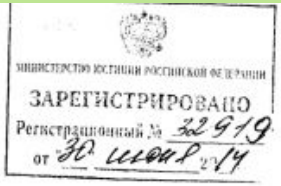
О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Глава 1. Общие положения

Статья 1. Сфера действия настоящего Федерального закона

Статья 17 Настоящий Федеральный закон вступает в силу с 1 января 2015 года.

Приказ ФСТЭК России от 14 марта 2014 г. № 31



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«14» марта 2014 г. Москва № 31

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

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 52, ст. 7137),
П Р И К А З Ы В А Ю:

Утвердить прилагаемые Требования 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.

ДИРЕКТОР ФЕДЕРВЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМЙ КОНТРОЛЮ

В.СЕЛИН

Приказ ФСТЭК России от 14 марта 2014 г. № 31
Нарушения Операторов

10. Для обеспечения защиты информации в автоматизированной системе управления оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

13.2. Классификация автоматизированной системы управления проводится заказчиком или оператором в зависимости от уровня значимости (критичности) информации, обработка которой осуществляется в автоматизированной системе управления.

Устанавливаются три класса защищенности автоматизированной системы управления, определяющие уровни защищенности автоматизированной системы управления. Самый низкий класс – третий, самый высокий – первый.

Результаты классификации автоматизированной системы управления оформляются актом классификации.

ФСТЭК России
ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
от 25 июля 2014 г. N 240/22/2748

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
от 25 июля 2014 г. N 240/22/2748

ПО ВОПРОСАМ
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
В КЛЮЧЕВЫХ СИСТЕМАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В СВЯЗИ
С ИЗДАНИЕМ ПРИКАЗА ФСТЭК РОССИИ ОТ 14 МАРТА 2014 Г. N 31
"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"

Сообщение ФСТЭК России от 25 июля 2014 г. N 240/22/2748. Нарушения Операторов

Автоматизированные системы 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, рассматриваются как один из классов ключевых систем информационной инфраструктуры, обладающий отдельными характерными особенностями.

Автоматизированные системы управления производственными и технологическими процессами подлежат отнесению к соответствующему уровню важности в соответствии с утвержденной системой признаков и включаются в реестр ключевых систем информационной инфраструктуры в порядке, установленном Положением о реестре ключевых систем информационной инфраструктуры (приказ ФСТЭК России от 4 марта 2009 г. N 74).

Лицензионные требования

ПРАВИТЕЛЬСТВО РОССИИСКОИ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ
от 13 июня 2012 г. N 581

О ЛИЦЕНЗИРОВАНИИ
РАЗРАБОТКИ, ПРОИЗВОДСТВА, ИСПЫТАНИЯ,
УСТАНОВКИ, МОНТАЖА, ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ, РЕМОНТА,
УТИЛИЗАЦИИ И РЕАЛИЗАЦИИ ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ

5. Лицензионными требованиями, предъявляемыми к соискателю лицензии (лицензиату) на осуществление разработки, производства, испытания, установки, монтажа, технического обслуживания, ремонта, утилизации и реализации вооружения и военной техники, являются:

г) наличие системы менеджмента качества, созданной и функционирующей согласно требованиям стандартов ИСО 9000 и государственных военных стандартов;

ГОСУДАРСТВЕННЫЙ ВОЕННЫЙ СТАНДАРТ

ГОСТ РВ 0015 — 002 — 2012

Система разработки и постановки на производство военной техники

СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА

Общие требования

4.3 Обеспечение информационной безопасности

4.3.1 В организации должен быть определен и документально оформлен порядок организации и выполнения работ по защите информации об образцах военной продукции, учитывающий характер и условия выполнения оборонного заказа при несанкционированном воздействии на информацию, циркулирующую в технических каналах. Организация, содержание и документация должны соответствовать требованиям ГОСТ Р 50739, ГОСТ РВ 50859, ГОСТ РВ 50934.

4.3.2 В организации должно быть определено подразделение (ответственный), осуществляющее менеджмент информационной безопасности на всех этапах жизненного цикла военной продукции.

4.3.3 При наличии соответствующих требований в контрактах (договорах) в организации должен быть определен и документально оформлен порядок выполнения работ по обеспечению информационной безопасности в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001.

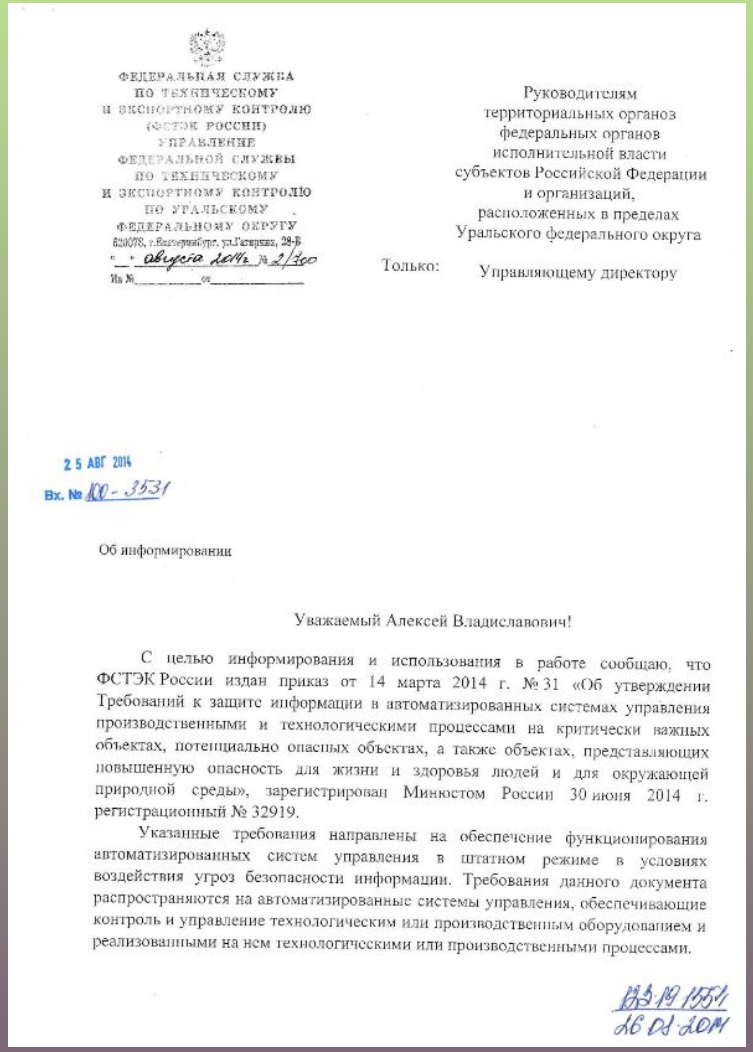
Письмо Минпромторга России от 14.02.14 № 16-791

В соответствии с поручением Заместителя Председателя Правительства Российской Федерации Д.О. Рогозина от 22 января 2014 г. № РД-П7-40с Департамент промышленности обычных вооружений, боеприпасов и спецхимии Минпромторга России доводит предложения ФСТЭК России по защите открытой технологической информации, циркулирующей в системах управления станков с ЧПУ.

В ходе проведенных проверок ФСТЭК России выявил типовые недостатки которые могут привести к нарушению целостности указанной информации и блокированию доступа к ней.

С Учетом изложенного представляется целесообразным провести дополнительный анализ информации, циркулирующей в системах управления станков, в целях уточнения степени ее секретности или относимости к информации ограниченного доступа. При необходимости, реализовать комплекс мер по защите такой информации в соответствии с требованиями нормативных правовых актов ФСТЭК России в этой области.

Письмо Управления ФСТЭК по Уральскому федеральному округу № 2/700 август 2014 г.



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)
УПРАВЛЕНИЕ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ
ПО УРАЛЬСКОМУ
ФЕДЕРАЛЬНОМУ ОКРУГУ
620078, г.Екатеринбург, ул.Гагарина, 28-Б
"__" августа 2014 № 2/700
На №_____от_____

Руководителям
территориальных органов
федеральных органов
исполнительной власти
субъектов Российской Федерации
и организаций,
расположенных в пределах
Уральского федерального округа

Только: Управляющему директору

25 АВГ 2014
Вх. № КО-3531

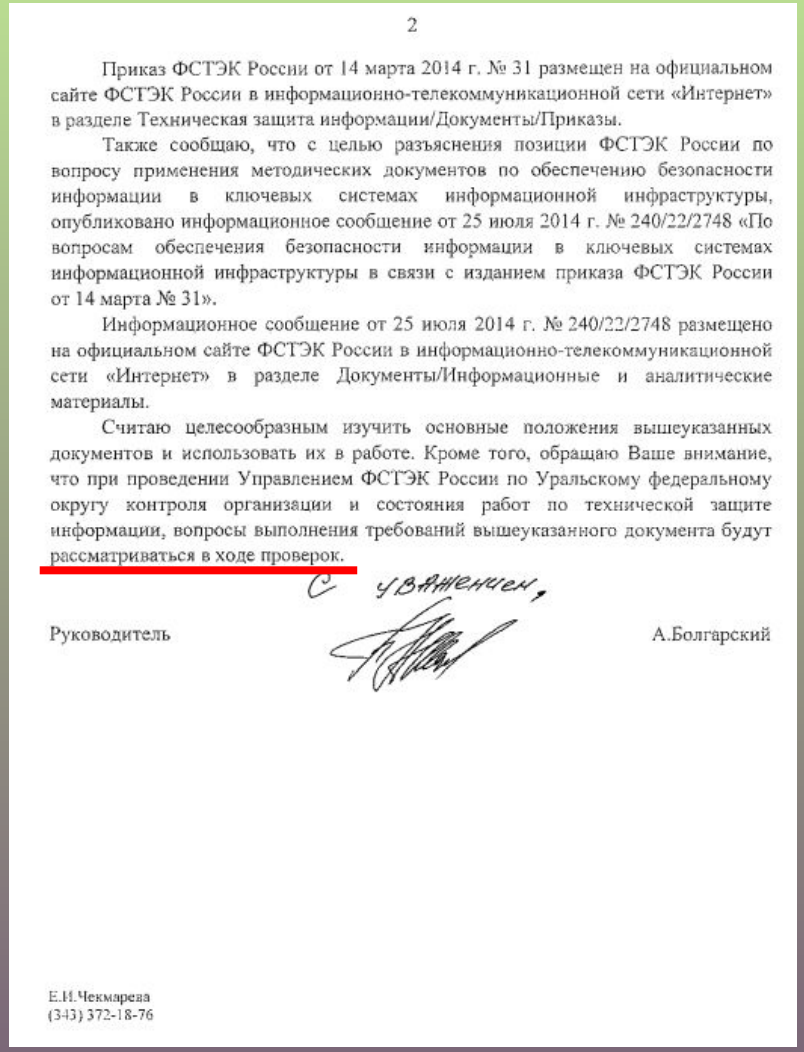
Об информировании

Уважаемый Алексей Владиславович!

С целью информирования и использования в работе сообщаю, что ФСТЭК России издан приказ от 14 марта 2014 г. № 31 «Об утверждении Требований к защите 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», зарегистрирован Минюстом России 30 июня 2014 г. регистрационный № 32919.

Указанные требования направлены на обеспечение функционирования автоматизированных систем управления в штатном режиме в условиях воздействия угроз безопасности информации. Требования данного документа распространяются на автоматизированные системы управления, обеспечивающие контроль и управление технологическим или производственным оборудованием и реализованными на нем технологическими или производственными процессами.

ВВ-19-1954
26.08.2014



Приказ ФСТЭК России от 14 марта 2014 г. № 31 размещен на официальном сайте ФСТЭК России в информационно-телекоммуникационной сети «Интернет» в разделе Техническая защита информации/Документы/Приказы.

Также сообщаю, что с целью разъяснения позиции ФСТЭК России по вопросу применения методических документов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, опубликовано информационное сообщение от 25 июля 2014 г. № 240/22/2748 «По вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14 марта № 31».

Информационное сообщение от 25 июля 2014 г. № 240/22/2748 размещено на официальном сайте ФСТЭК России в информационно-телекоммуникационной сети «Интернет» в разделе Документы/Информационные и аналитические материалы.

Считаю целесообразным изучить основные положения вышеуказанных документов и использовать их в работе. Кроме того, обращаю Ваше внимание, что при проведении Управлением ФСТЭК России по Уральскому федеральному округу контроля организации и состояния работ по технической защите информации, вопросы выполнения требований вышеуказанного документа будут рассматриваться в ходе проверок.

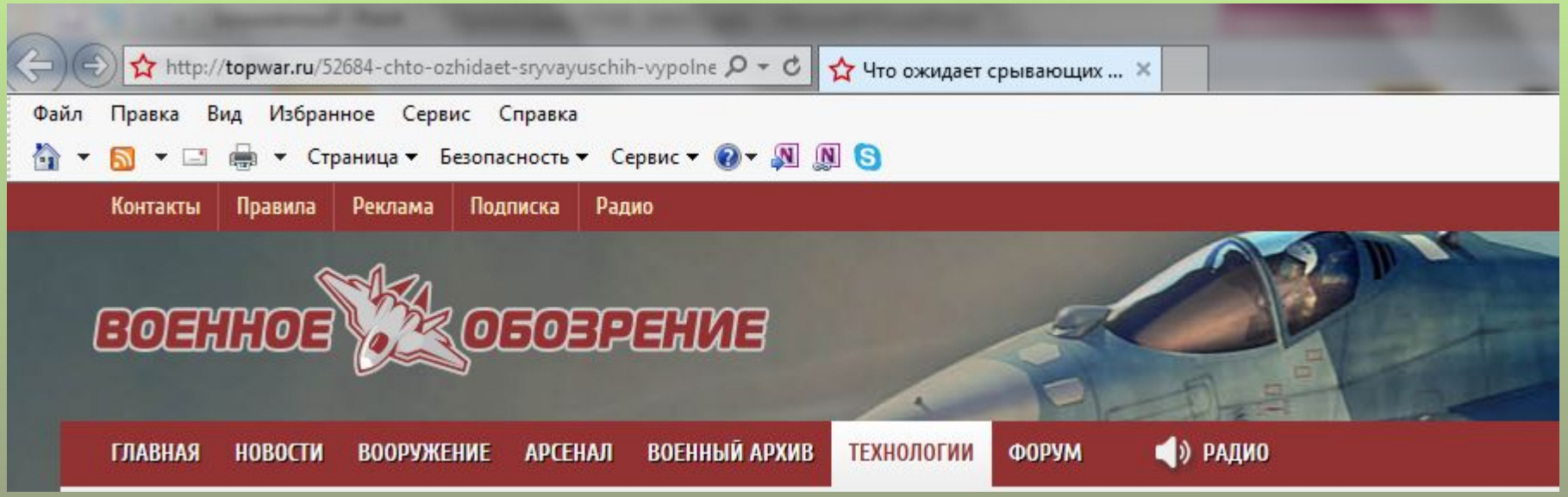
С уважением,

Руководитель А.Болгарский

Е.И.Чекмарева
(343) 372-18-76

4 Риски нарушения непрерывности бизнеса

Обязательность выполнение гособоронзаказа

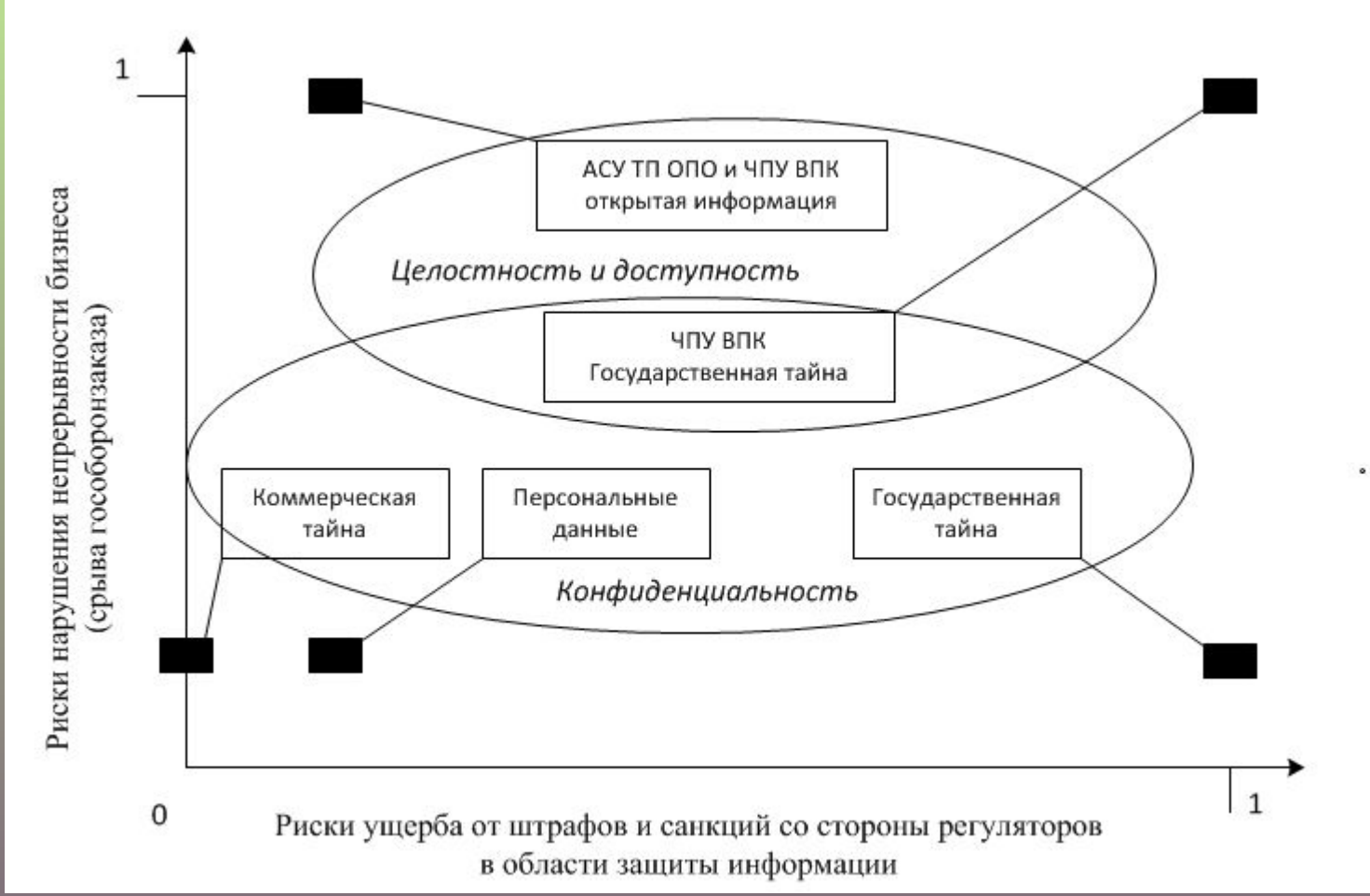


Что ожидает срывающих выполнение гособоронзаказа?

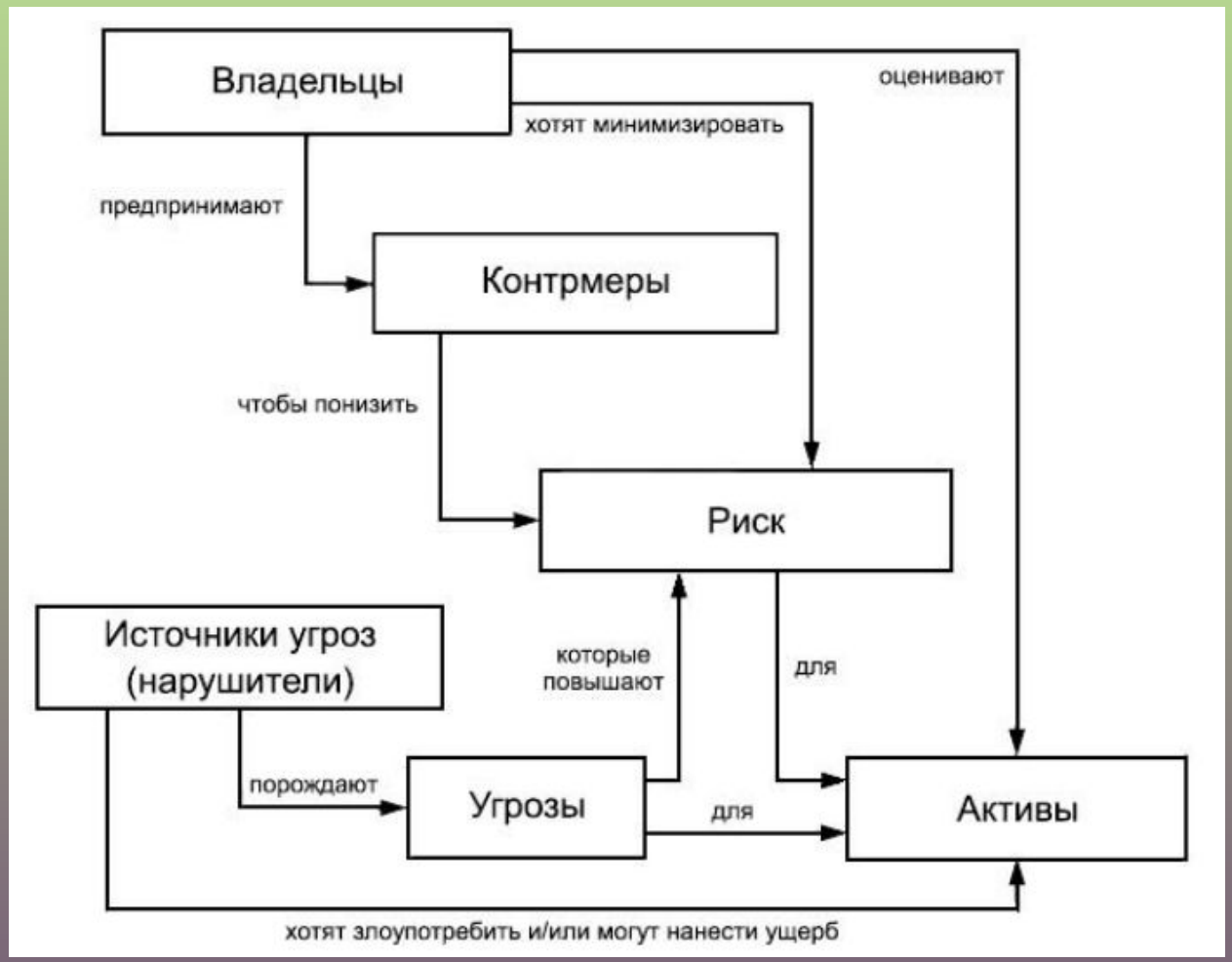
24 июня 2014 Распечатать

На фоне сведений о том, что в ближайшее время контроль выполнения государственного оборонного заказа, будет перераспределён между ФАС (Федеральной антимонопольной службой), Счётной палатой и специальной группой при Главной военной прокуратуре, на правительственном уровне выдвигаются идеи и по поводу возможного наказания тех, кто причастен к срыву выполнения ГОЗ. Вице-премьер Дмитрий Рогозин, который курирует сферу ВПК, заявляет, что одно из наиболее вероятных наказаний – дисквалификация предприятий или их руководителей из системы реализации гособоронзаказа.

Особенности защиты информации в АСУ ТП и ЧПУ



Информационная технология
Методы и средства обеспечения безопасности
ГОСТы Р ИСО/МЭК серии 15408



Система менеджмента информационной безопасности (СМИБ)

СМИБ (information security management system; ISMS): Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Менеджмент риска информационной безопасности (ГОСТ Р ИСО/МЭК 27005-2010)

Риск информационной безопасности (information security risk): Возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Активом является что-либо, имеющее ценность для организации и, следовательно, нуждающееся в защите.

Для установления ценности активов организация должна в первую очередь определить все свои активы на соответствующем уровне детализации.

Могут различаться два вида активов:

- основные активы, включающие бизнес-процессы, бизнес-деятельность и информацию;

- вспомогательные (поддерживающие) активы, от которых зависят основные составные части области применения всех типов, включающие аппаратные средства, программное обеспечение, сеть, персонал, место функционирования организации, структуру организации.

Оценка и обработка рисков информационной безопасности (ГОСТ Р ИСО/МЭК 27005-2010)

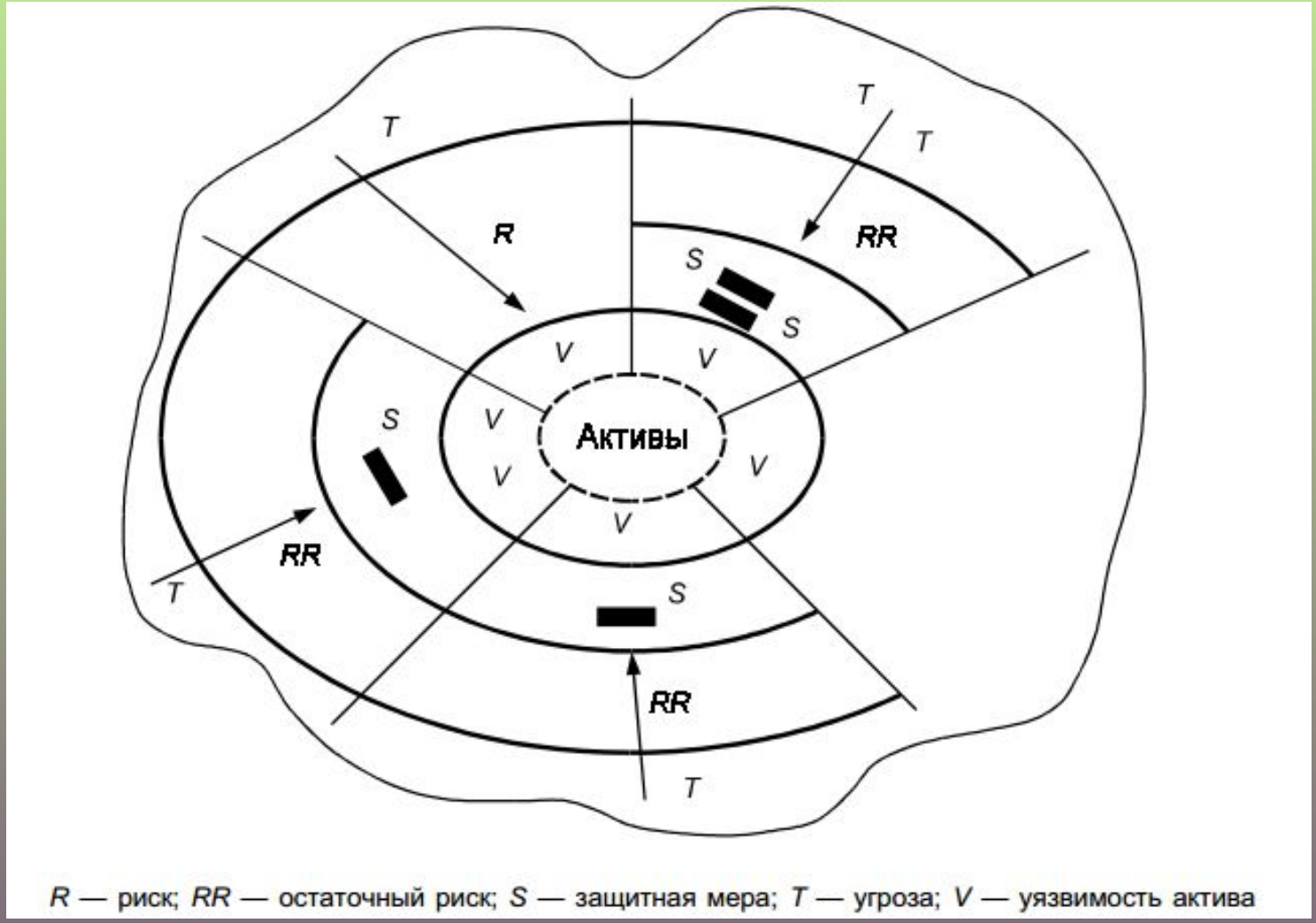
В процессе оценки риска устанавливается ценность информационных активов, выявляются потенциальные угрозы и уязвимости, которые существуют или могут существовать, определяются существующие меры и средства контроля и управления и их воздействие на идентифицированные риски, определяются возможные последствия и, наконец, назначаются приоритеты установленным рискам, а также осуществляется их ранжирование
по критериям оценки риска, зафиксированным при установлении контекста.

Цель идентификации риска - определить, что могло бы произойти при нанесении возможного ущерба, и получить представление о том, как, где и почему мог иметь место этот ущерб.

Решения, связанные с оценкой риска, обычно основываются на приемлемом уровне риска

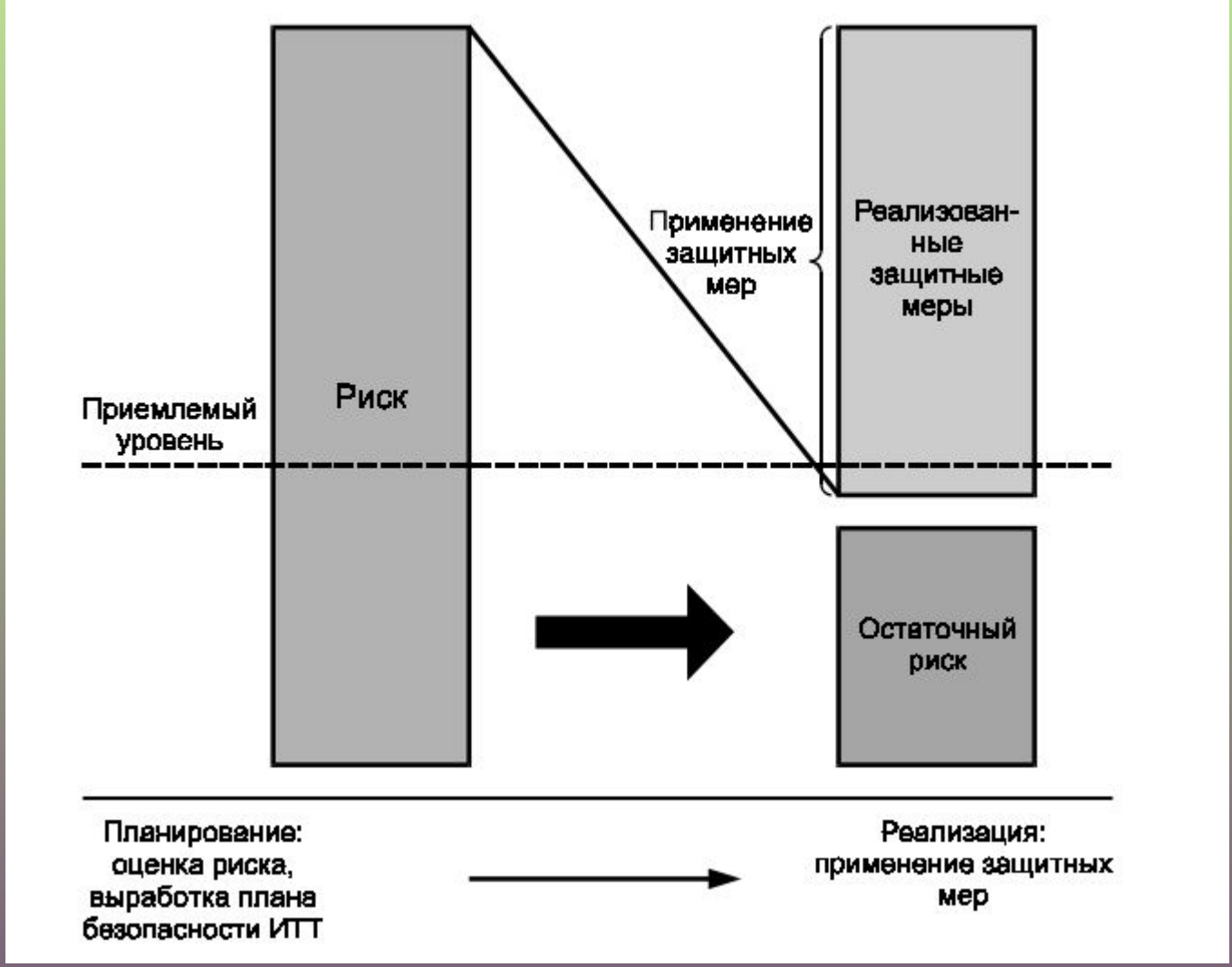
Должны реализовываться такие варианты, при которых значительное снижение риска может быть достигнуто при относительно небольших затратах.

Взаимосвязь компонентов безопасности

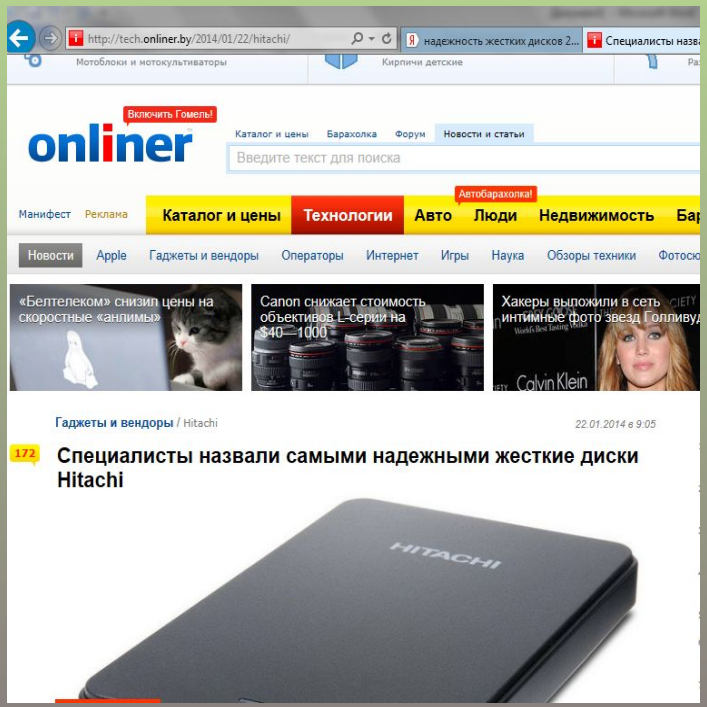


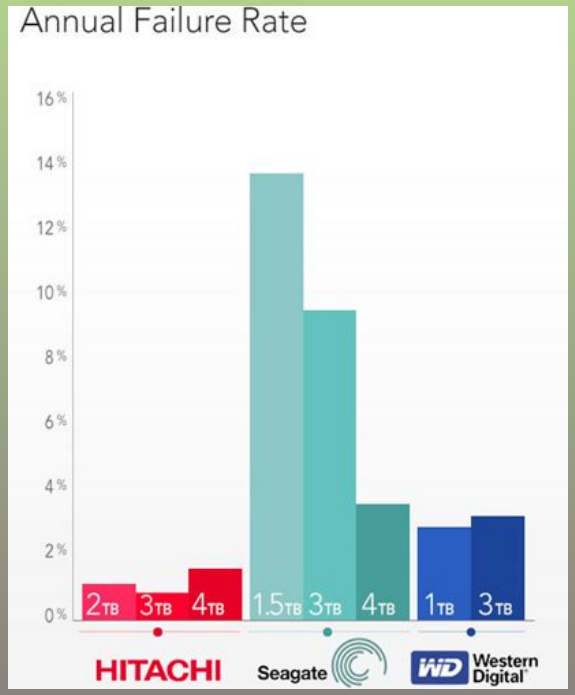
R — риск; *RR* — остаточный риск; *S* — защитная мера; *T* — угроза; *V* — уязвимость актива

Взаимосвязь защитных мер и риска



Оценка возможности (вероятности) угрозы нарушения доступности информации в результате дефектов, сбоев, отказов и аварий технических средств и систем оборудования АСУ ТП и ЧПУ





Вероятность отказов в течении одного года – 3%

Вероятность (частота реализации) сценария нарушения доступности информации в результате дефектов, сбоев, отказов и аварий технических средств $3*10^{-2}$ в год (один раз в 30 лет)

Оценка возможности (вероятности) угрозы нарушения доступности информации в результате пожара в серверном помещении

Приложение
к приказу МЧС России
от 30.06.2009 № 382

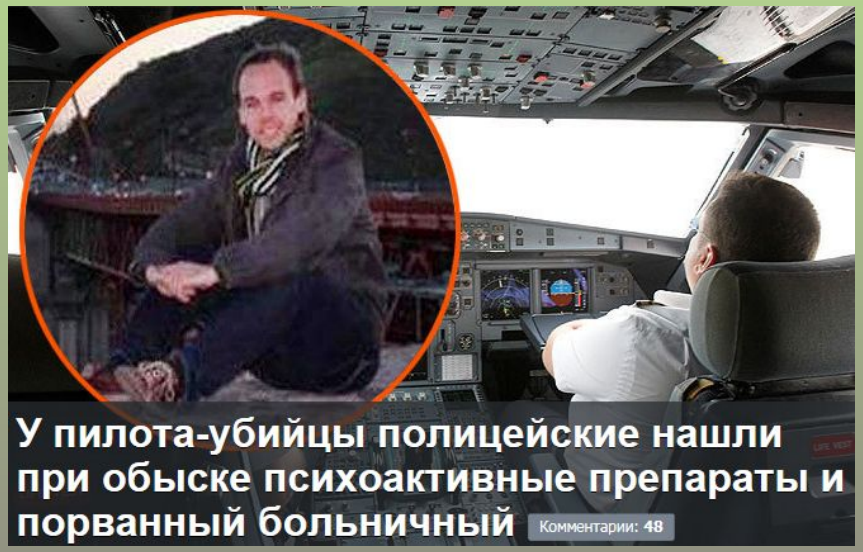
МЕТОДИКА
определения расчетных величин пожарного риска в зданиях, сооружениях и строениях различных классов функциональной пожарной опасности

Вероятность пожара в серверном помещении в течении одного года – $4*10^{-2}$

При возникновении пожара в серверном помещении АСУ ТП ПУТ в 95 случаях из 100 он будет локализован.

Вероятность (частота реализации) сценария нарушения доступности информации в результате пожара в серверном помещении не превышает величины $4*10^{-2}* 5*10^{-2}= 2*10^{-3}$ в год (один раз в 500 лет)

Оценка возможности (вероятности) угрозы нарушения целостности и доступности информации в результате действий неадекватных лиц – «пилоты-самоубийцы»



Оценочные данные ВОЗ по абсолютному и относительному числу самоубийств за 2012 г[1]

№ (2012)	Государство (достоверность*)	Число самоубийств абсолютное за 2012 г. всего (женщин / мужчин)	Число самоубийств** на 100 000 чел. за 2012 г. всего (женщин / мужчин)	Число самоубийств** на 100 000 чел. за 2000 г. всего (женщин / мужчин)
1	Гайана (2)	277 (72 / 205)	44,2 (22,1 / 70,8)	48,3 (24,6 / 72,2)
2	КНДР (4)	9790 (4828 / 4962)	38,5 (35,1 / 45,4)	47,3 (41,3 / 58,2)
3	Республика Корея (1)	17908 (5755 / 12153)	28,9 (18,0 / 41,7)	13,8 (8,1 / 20,4)
4	Шри-Ланка (2)	6170 (1446 / 4724)	28,8 (12,8 / 46,4)	52,7 (22,3 / 84,1)
5	Литва (1)	1007 (177 / 830)	28,2 (8,4 / 51,0)	44,9 (15,0 / 79,3)
6	Суринам (1)	145 (32 / 114)	27,8 (11,9 / 44,5)	19,8 (9,7 / 29,7)
7	Мозамбик (4)	4360 (1639 / 2721)	27,4 (21,1 / 34,2)	24,6 (19,1 / 30,9)
8	Непал (4)	5572 (2468 / 3104)	24,9 (20,0 / 30,1)	33,5 (27,1 / 40,5)
9	Танзания (4)	7228 (2445 / 4783)	24,9 (18,3 / 31,6)	23,8 (18,6 / 29,1)
10	Казахстан (1)	3912 (788 / 3123)	23,8 (9,3 / 40,6)	37,6 (12,6 / 66,9)
11	Бурунди (4)	1617 (401 / 1216)	23,1 (12,5 / 34,1)	19,6 (10,3 / 29,6)
12	Индия (3)	258075 (99977/158098)	21,1 (16,4 / 25,8)	23,3 (20,3 / 26,2)
13	Южный Судан (4)	1470 (443 / 1027)	19,8 (12,8 / 27,1)	20,8 (12,9 / 28,9)
14	Туркмения (2)	1003 (197 / 806)	19,6 (7,5 / 32,5)	15,2 (7,0 / 24,0)
15	Россия (1)	31997 (5781 / 26216)	19,5 (6,2 / 35,1)	35,0 (9,6 / 64,3)

Вероятность «суицида» высококвалифицированного специалиста – $2*10^{-4}$

При «суициде» в 1 случае из 100 специалист реализует его в отношении АСУ ТП и ЧПУ

При наличии 5 высококвалифицированных специалистов вероятность (частота реализации) сценария нарушения целостности и доступности информации в результате действий неадекватных лиц («пилотов-самоубийц»)

$2*10^{-4}* 1*10^{-2}*5= 1*10^{-5}$ в год (один раз в 100 тысяч лет)

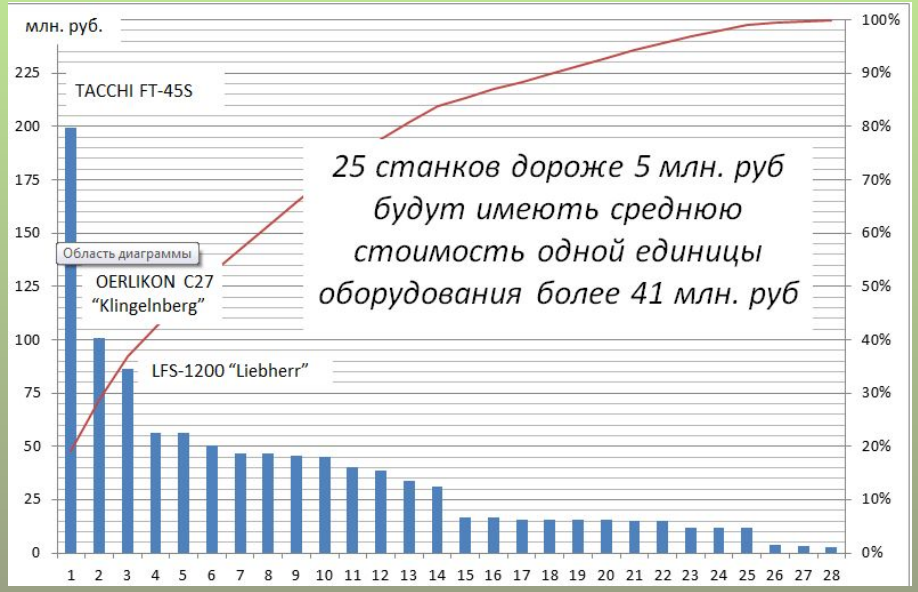
Оценка возможности (вероятности) угрозы нарушения целостности и доступности информации в результате компьютерной атаки типа «Stuxnet»

С учетом того, что после 2010 г. достоверных фактов проведения подобных компьютерных атак не установлено, выборочная частота реализации подобного сценария составляет величину – один раз в пять лет на все АСУ ТП во всем мире

С учетом уровня автоматизации России, уровня автоматизации металлургии в России, доли комбината в общем объеме металлургического производства России и с учетом того, что на комбинате эксплуатируется более 100 АСУ ТП -

вероятность (частота реализации) сценария нарушения целостности и доступности информации в результате атаки типа «Stuxnet» на дну АСУ ТП, не превышает величины $1*10^{-6}$ в год (один раз в миллион лет)

Потенциально возможный ущерб и риски на примере оборонного предприятия



Стоимость единицы оборудования с ЧПУ – 40 млн. руб.

Срок окупаемости – 8,3 года

Чистая прибыль от эксплуатации единицы оборудования с ЧПУ в течении одного года – 40/8,3=4,8 млн. руб.

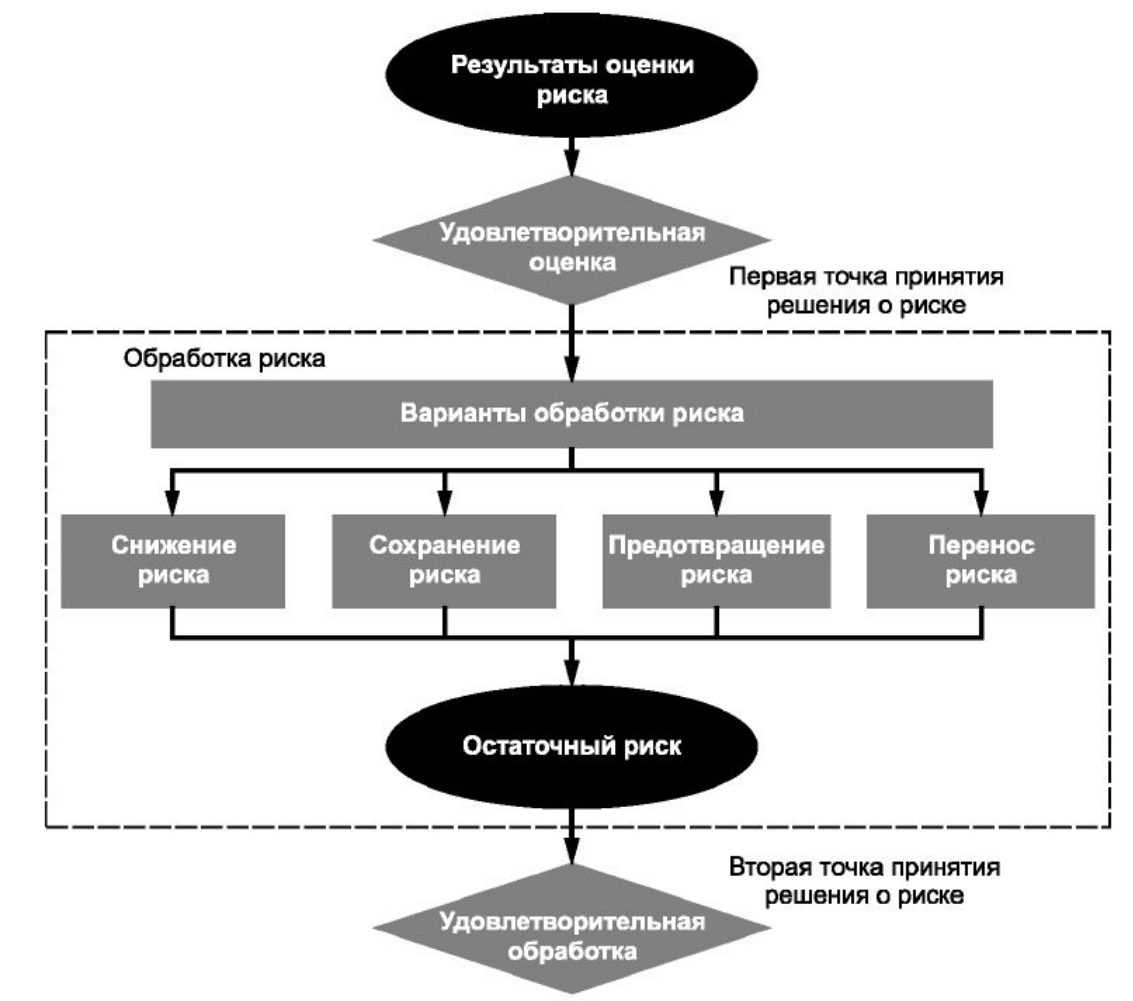
*Потери (упущенная прибыль) от простоя единицы оборудования с ЧПУ в течении шести месяцев – (4,8/12)*6=2,4 млн. руб.*

Вероятность (частота реализации) сценария нарушения доступности информации в результате отказов технических средств (ТС) - один раз в 30 лет

Риск от отказа ТС на единице оборудования – 80 тыс. руб. в год

Риск от отказа ТС на 50 единицах оборудования – 4 млн. руб. в год

Обработка риска



Обработка риска - снижение риска

на примере системы ЧПУ SINUMERIK 840D sl

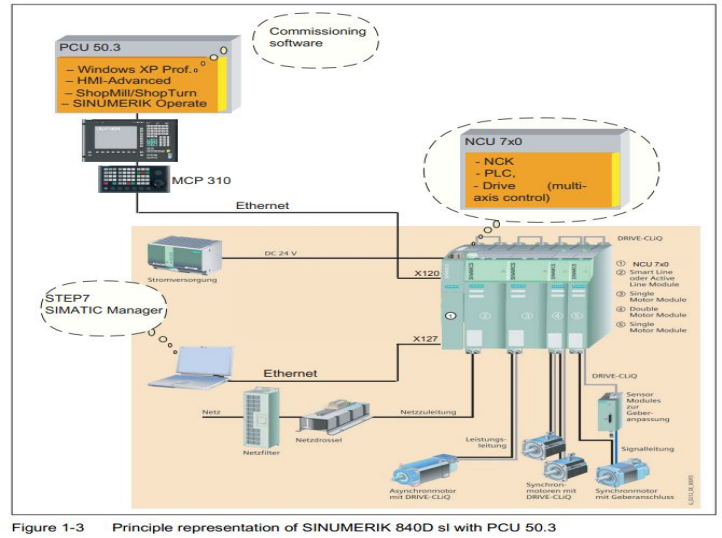
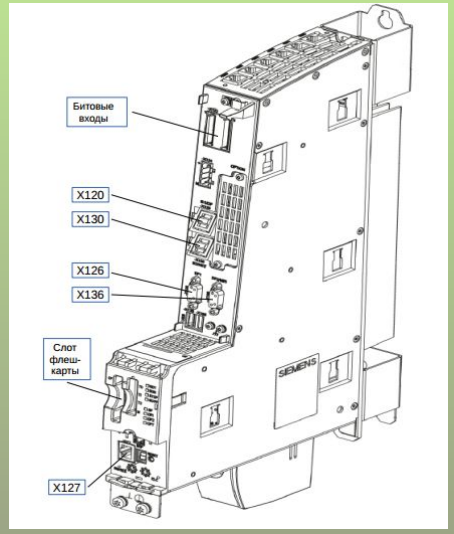


Figure 1-3 Principle representation of SINUMERIK 840D sl with PCU 50.3

+

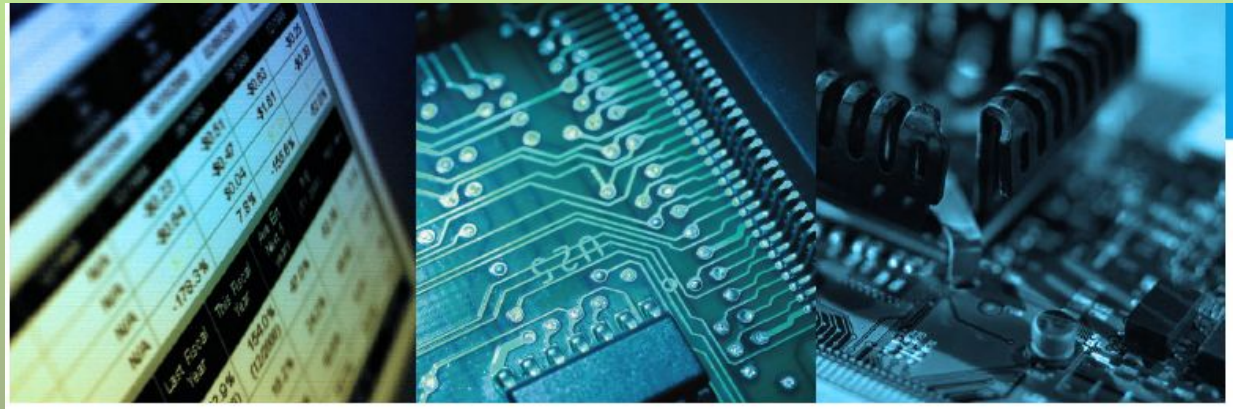


Система ЧПУ SINUMERIK 840D sl + ЗИП Модуль NCU 7x0.3

Вероятность (частота реализации) сценария нарушения доступности информации в результате отказа одного модуля NCU 7x0.3
$3*10^{-2}$ в год (один раз в 30 лет)

Вероятность (частота реализации) сценария нарушения доступности информации в результате одновременного отказа сразу дух модулей NCU 7x0.3 (основного и резервного)
$3*10^{-2} * 3*10^{-2} = 9*10^{-4}$ в год (один раз в тысячу лет)

Обработка риска – перенос риска
Страхование риска



Программа страхования кибер-рисков CyberEdge℠

1. Кибер-риски (риски операторов данных) возникают в результате ежедневной работы с информацией и информационными системами. От каких рисков защищает программа страхования CyberEdge℠?

Обязательные секции полиса		
Покрытие A	**Покрытие B**	**Покрытие C**
Ответственность за нарушение персональных данных и корпоративной информации (коммерческие тайны, профессиональная информация, бюджеты, перечни клиентов и пр.) по причине несанкционированного раскрытия или передачи, в том числе заражения вирусами, уничтожения, модификации или удаления информации, физической кражи или утери аппаратного обеспечения и пр.	Покрытие расходов при административном расследовании в отношении данных со стороны регулирующих органов.	Расходы на программно-техническую экспертизу, позволяющую установить причину утечки; Расходы на восстановление репутации компании и /или ее должностных лиц; Расходы на уведомление субъектов данных и мониторинг; Расходы на восстановление электронных данных.

Дополнительные покрытия		
Покрытие D	**Покрытие E**	**Покрытие F**
Ответственность за содержание информации	Виртуальное вымогательство	Убытки от сбоев в работе сети в результате нарушения функционирования системы безопасности, компенсация недополученной прибыли.

5 Два подхода к защите информации в АСУ ТП и общие рекомендации

Общие аспекты защиты информации в АСУ ТП

Бизнес-процессы, реализуемые с использованием информационных технологий, относятся к наиболее ценным активам промышленного предприятия.

Угрозы информационным активам постоянно возрастают. Новым серьезным источником угроз информационной безопасности является применения «информационного оружия».

Требования по обеспечению информационной безопасности к операторам автоматизированных систем управления производственными и технологическими процессами со стороны регуляторов будут существенно повышены.

Методическая и нормативная база ФСТЭК России и ФСБ России по защите информации на оборудовании с ЧПУ находится в стадии разработки.

Техническая защита или обеспечение безопасности

Техническая защита (*конфиденциальной*) информации	**Обеспечение безопасности информации**
Цель	
Устранить нарушения требований регуляторов в области защиты информации (*31 Приказ ФСТЭК России, документы по КСИИ*)	Обеспечить непрерывность бизнеса (*ГОСТы Р серии 53647 «Менеджмент непрерывности бизнеса»*) и повысить безопасность используемых информационных технологий (*ГОСТы Р ИСО/МЭК серии 15408 «Информационная технология. Методы и средства обеспечения безопасности»*)
Задача	
Снизить внешние риски – риски ущерба от штрафов и санкций со стороны регуляторов в области защиты информации.	Снизить риски ущерба для бизнеса (*ГОСТ Р ИСО 31000, ГОСТы Р серии 51901 -Менеджмент риска*)
Этапы	
Разработать модель угроз *от несанкционированного доступа к* информации (*базовые модели по КССИ и ЧПУ, проект ГОСТ технического комитета ТК 362 «Угрозы безопасности. Общие положения», план 2015 г.*) и качественно (*экспертным методом*) оценить их актуальность (*методика по КСИИ*)	Разработать полную модель угроз от всех возможных их источников: антропогенных, техногенных и природных (*ГОСТ Р 51275-2006 Факторы, воздействующие на информацию, базовая модель КСИИ и ГОСТ Р ИСО/МЭК 27005 - Менеджмент риска информационной безопасности*)
Сформировать требования к системе защиты информации, исходя из установленного (максимально заниженного) класса (уровня) защищенности (*31 Приказ ФСТЭК России, требования по КСИИ*)	На основе методов сценарного анализа количественно оценить риски по всем угрозам для наиболее ценных активов и определить те затраты, которые экономически оправданы для их снижения
Закупить, установить и настроить технические средства защиты информации (цена определяются их рыночной стоимостью и, если на это будут выделены бюджеты, то затраты могут оказаться экономически нецелесообразными)	Обосновать бюджеты и добиться их утверждения. С учетом выделенных ресурсов, сформировать поэтапный план наиболее рационального их использования (*в случае отказа в финансировании, вся ответственность за возможные аварии - на лицах, принявших данное решение*)
Аттестовать объект информатизации (или провести проверку его соответствия требованиям по защите информации)	Разработать, внедрить и сертифицировать (постоянно поддерживать) систему менеджмента информационной безопасности (*ГОСТы Р ИСО/МЭК серии 27000*)

Снижение рисков штрафов и санкций со стороны регуляторов в области защиты информации

10. Для обеспечения защиты информации в автоматизированной системе управления оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

Ответственный должен иметь допуск для работы со сведениями, составляющими государственную тайну (КСИИ – система признаков)

13.2. Классификация автоматизированной системы управления проводится заказчиком или оператором в зависимости от уровня значимости (критичности) информации, обработка которой осуществляется в автоматизированной системе управления.

Приказом руководителя создать комиссию, которая в своей работе руководствуется Постановлением Правительства от 21 мая 2007 г. N 304

Результаты классификации автоматизированной системы управления оформляются актом классификации.

Автоматизированные системы управления производственными и технологическими процессами подлежат отнесению к соответствующему уровню важности в соответствии с утвержденной системой признаков и включаются в реестр ключевых систем информационной инфраструктуры в порядке, установленном Положением о реестре ключевых систем информационной инфраструктуры (приказ ФСТЭК России от 4 марта 2009 г. N 74).

Для подготовки шаблонов документов целесообразно привлечь специализированную организацию

Екатеринбургский НТЦ ФГУП «НПП «Гамма»

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

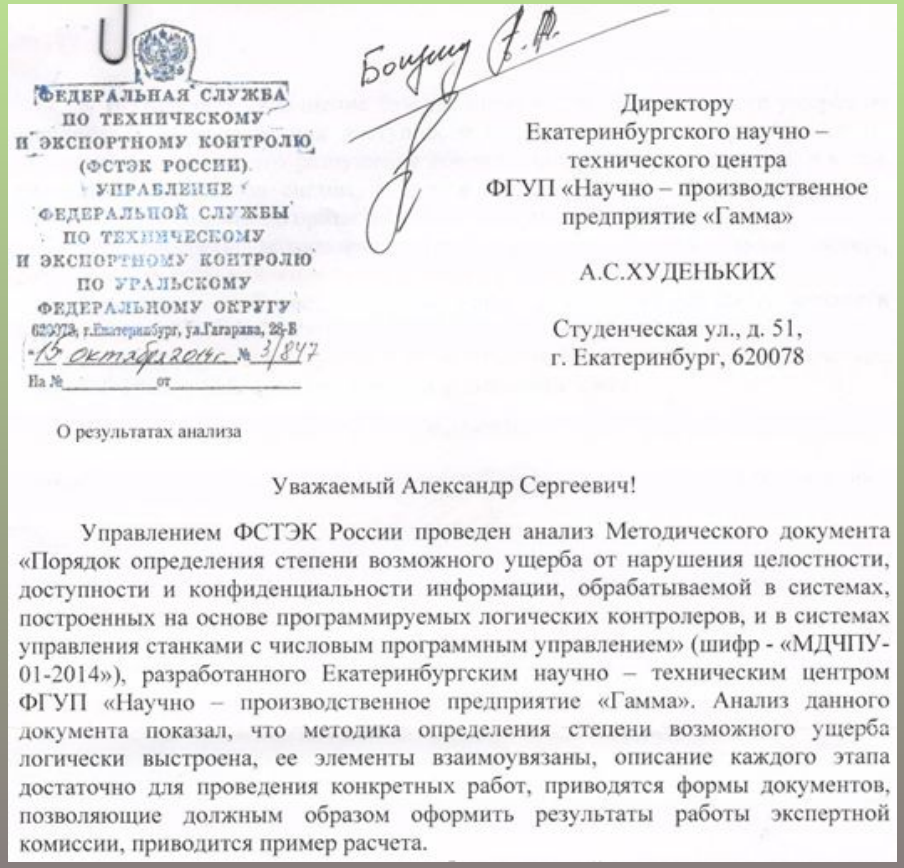
КООРДИНАЦИОННО-МЕТОДИЧЕСКИЙ СОВЕТ ПО ПРОБЛЕМАМ ПРОТИВОДЕЙСТВИЯ ИНОСТРАННЫМ ТЕХНИЧЕСКИМ РАЗВЕДКАМ И ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЙ ОБОРОННЫХ ОТРАСЛЕЙ ПРОМЫШЛЕННОСТИ УРАЛЬСКОГО ФЕДЕРАЛЬНОГО ОКРУГ

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

Порядок определения степени возможного материального ущерба от нарушения целостности, доступности и конфиденциальности информации, обрабатываемой в системах, построенных на основе программируемых логических контроллеров, и в системах управления станками с числовым программным управлением

Шифр – «МДЧПУ-01-2014»

Апробация методического документа



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)
УПРАВЛЕНИЕ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ
ПО УРАЛЬСКОМУ
ФЕДЕРАЛЬНОМУ ОКРУГУ
620078, г.Екатеринбург, ул.Гагарина, 28-Б
15 октября 2014г. № 3/847
На №_____от_____

Директору
Екатеринбургского научно –
технического центра
ФГУП «Научно – производственное
предприятие «Гамма»

А.С.ХУДЕНЬКИХ

Студенческая ул., д. 51,
г. Екатеринбург, 620078

О результатах анализа

Уважаемый Александр Сергеевич!

Управлением ФСТЭК России проведен анализ Методического документа «Порядок определения степени возможного ущерба от нарушения целостности, доступности и конфиденциальности информации, обрабатываемой в системах, построенных на основе программируемых логических контролеров, и в системах управления станками с числовым программным управлением» (шифр - «МДЧПУ-01-2014»), разработанного Екатеринбургским научно – техническим центром ФГУП «Научно – производственное предприятие «Гамма». Анализ данного документа показал, что методика определения степени возможного ущерба логически выстроена, ее элементы взаимоувязаны, описание каждого этапа достаточно для проведения конкретных работ, приводятся формы документов, позволяющие должным образом оформить результаты работы экспертной комиссии, приводится пример расчета.

Контактный телефон должностного лица, ответственного за взаимодействие (343) 372-18-60 – Забокрицкий Александр Александрович.

С уважением,

Руководитель А.Болгарский

УВЗ ЗАВОД №9

ДОГОВОР от 1 июня 2014 г.№ 19/14-у/590-2/7/2636
ДОГОВОР от 1 октября 2014 г. № 34/14-у/590-2/9/
Приказ Генерального директора от 14 ноября 2014 г. №287

Совет предприятий оборонных отраслей промышленности Свердловской области

Заседание Совета главных инженеров (главных технических специалистов) предприятий ОПК Уральского региона 23 октября 2014 г.

СТАРТ
ОАО « НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ
«СТАРТ» им. А.И. ЯСКИНА»

6 ноября 2014 г.

ОПЫТНОЕ КОНСТРУКТОРСКОЕ БЮРО ИМ. ЛЮЛЬЕВА Л.В
НОВАТОР

19 ноября 2014 г.

12-13 ноября 2014
КОСМИЧЕСКИЕ И ИНФОРМАЦИОННЫЕ
ТЕХНОЛОГИИ XXI ВЕКА
sit
МЕЖДУНАРОДНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ КОНГРЕСС

Информационное письмо от 8.04.2015 г. № 04-106

**СОЮЗ ПРЕДПРИЯТИЙ
ОБОРОННЫХ ОТРАСЛЕЙ ПРОМЫШЛЕННОСТИ
СВЕРДЛОВСКОЙ ОБЛАСТИ**

620027, г. Екатеринбург, ул. Луначарского, 31, т/ф (343) 355-02-09, 354-27-27, 354-32-70
E-mail:souzop@ural.ru , http://www.souzop.ru

08.04.2015г. № 04- 106

Руководителю предприятия

На _____ от _____

О вопросах обеспечения безопасности информации в АСУ ТП и станках с ЧПУ

Уважаемые коллеги!

Считаем целесообразным довести до сведения руководителей предприятий оборонных отраслей промышленности Уральского федерального округа, а также других заинтересованных сторон о том, что совместным Решением Координационно-методического Совета по проблемам противодействия иностранным техническим разведкам и технической защиты информации предприятий оборонных отраслей промышленности Уральского федерального округа (КМС ПД ИТР и ТЗИ ОПК УрФО) и Совета главных специалистов информационно-коммуникационных технологий Союза предприятий оборонных отраслей промышленности Свердловской области (протокол от 27 ноября 2014 г.) с учетом замечаний, сформулированных Управлением Федеральной службы по техническому и экспортному контролю по Уральскому федеральному округу в письме на имя директора ЕНТЦ ФГУП «НПП «Гамма» (исх. №3/847 от 15.10.2014г.), утвержден и введен в действие Методический документ МДЧПУ-01-2014 «Порядок определения степени возможного материального ущерба от нарушения целостности, доступности и конфиденциальности информации, обрабатываемой в системах, построенных на основе программируемых логических контроллеров, и в системах управления станками с числовым программным управлением» (далее – методический документ).

Данный методический документ разработан Екатеринбургским научно-техническим центром федерального государственного унитарного предприятия «Научно-производственное предприятие «Гамма» (далее - ЕНТЦ ФГУП «НПП «Гамма») и Обществом с ограниченной ответственностью «Информбюро» (далее - ООО «Информбюро»).

Для получения Методического документа МДЧПУ-01-2014, а также всех необходимых консультационных услуг по его применению можно обращаться по следующей контактной информации:

Заплатин Алексей Владимирович, начальник Управления системных проектов ЕНТЦ ФГУП «НПП «Гамма», директор ООО «Информбюро», e-mail: zav@gammaural.ru, тел./факс (343) 375-49-31, моб.т. 8-912-60-02-664;

Бондин Андрей Рудольфович, начальник отдела сертификации ЕНТЦ ФГУП «НПП «Гамма», главный инженер ООО «Информбюро», e-mail: bondin@gammaural.ru, тел./факс (343) 375-49-31, моб. +7-912-24-85-061.

В случае необходимости разработки других методических документов, а также для получения комплекса различных специальных научно-технических услуг по защите информации, обрабатываемой в автоматизированных системах управления производственными и технологическими процессами, в системах, построенных на основе программируемых логических контроллеров, и в системах управления станками с числовым программным управлением, предлагаем обращаться в ЕНТЦ ФГУП «НПП «Гамма» и ООО «Информбюро».

Исполнительный директор Союза,
Секретарь КМС ПД ИТР и ТЗИ
ОПК УрФО В.А.Кукарских

Екатеринбургский НТЦ ФГУП «НПП «Гамма»

Защита информации на оборудовании с ЧПУ - уязвимости, угрозы и риски

Спасибо за внимание