КСБ-СОФТ

Информационная безопасность объектов КИИ – от категорирования до построения системы защиты и импортозамещения

Спикеры:

- **Шляпкин Максим** – начальник отдела защиты объектов КИИ и АСУ ТП, КСБ-СОФТ
- **Порошин Михаил** – менеджер по развитию бизнеса, QTECH

Модератор:

- **Суздальцев Андрей** – заместитель начальника отдела регионального развития, КСБ-СОФТ

Обменивайтесь
сообщениями во вкладке «Чат»

Запись вебинара направим
Всем участникам на указанный
при регистрации e-mail

Задавайте вопросы
во вкладке «Вопросы»

План вебинара

- Нюансы категорирования объектов КИИ: кто является субъектом КИИ, выделение объектов КИИ, определение категории значимости
- Проектирование системы защиты объектов КИИ
- Импортозамещение: особенности внедрения отечественного оборудования
- Ответы на вопросы

«КСБ-СОФТ»

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

70+
регионов внедрения

4000+
реализованных проектов

В 2023 году реализовано 35 проектов по обеспечению безопасности КИИ (категоривание, проектирование, внедрение, анализ уязвимостей/пентест, мониторинг)

Шаги определения субъекта КИИ

1. Определяются сферы деятельности организации, соответствующие 187-ФЗ на основании: ОКВЭД и ОКОГУ; лицензий, сертификатов и иных разрешительных документов на виды деятельности; учредительных документов, уставов, положений организации

2. Проводится инвентаризация ИС/АСУ/ИТКС организации и определение их назначения

3. Проводится анализ на предмет принадлежности ИС/АСУ/ИТКС организации на основании договоров, контрактов на приобретения прав собственности либо аренды.

4. Определяются ИС/АСУ/ИТКС, используемые для реализации соответствующего вида деятельности, указанного в уставе, лицензии или ОКВЭД организации, а также их принадлежности к сфере деятельности из 187-ФЗ

ВАЖНО: Данный шаг не регламентирован в НПА. На основании данного шага можно определить только признаки того, что организация является субъектом КИИ

Министерства финансов РФ – **не** являются субъектами КИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)

Старая Басманная, д. 17, Москва, 105066
Тел., факс: (495) 696-49-04
E-mail: postin@fstec.ru

16.11.2022 № 240/

На №

М.С.ШЛЯПКИНУ
[redacted]

О разъяснении требований
федерального закона

Уважаемый Максим Сергеевич!

Согласно статье 2 Федерального закона от 26 июля 2017 г. № 187 - ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» субъектами критической информационной инфраструктуры являются государственные органы и государственные учреждения, осуществляющие деятельность в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, принадлежащие им на праве собственности, аренды или на ином законном основании, являются объектами критической информационной инфраструктуры.

Министерства финансов Российской Федерации не осуществляют деятельность ни в одной из указанных сфер (областей), следовательно, не относится к субъектам критической информационной инфраструктуры Российской Федерации.

Начальник 8 управления Е.Торбенко

Новая сфера в 187-ФЗ

Согласно Федеральному закону от 10 июля 2023 г. N 312-ФЗ "О внесении изменения в статью 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»:

- **субъекты критической информационной инфраструктуры** - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, **государственной регистрации прав на недвижимое имущество и сделок с ним**, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Какие объекты КИИ категорировать?

Требования НПА

Федеральный закон от 26 июля 2017 г. N 187-ФЗ

- Субъекты критической информационной инфраструктуры в соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присваивают одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам критической информационной инфраструктуры. Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий.

Постановление Правительства РФ от 8 февраля 2018 г. N 127

- Категорированию подлежат объекты критической информационной инфраструктуры, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

Требования НПА

Постановление Правительства РФ от 8 февраля 2018 г. N 127

- Категорирование включает в себя:

- а) определение процессов, указанных в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

- б) выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее - критические процессы);

- в) определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

- г) формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию (далее - перечень объектов);

- д) оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

- е) присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

Методические рекомендации

по категорированию объектов критической информационной инфраструктуры

сферы здравоохранения

2.8.1. Порядок формирования Перечня потенциально значимых объектов КИИ

51. ИС, ИТКС, АСУ считается потенциально значимым объектом КИИ организации сферы здравоохранения, если в результате анализа установлено, что она одновременно задействована в реализации критического бизнес-процесса и оказывает влияние на нарушение или прекращение критического бизнес-процесса.

52. ИС, ИТКС, АСУ не считается потенциально значимым объектом КИИ организации сферы здравоохранения и не требует присвоения одной из категорий значимости, установленной постановлением Правительства РФ от 08.02.2018 № 127, если в результате анализа установлено, что она не задействована в реализации критического бизнес-процесса организации сферы здравоохранения, либо она задействована в реализации критического бизнес-процесса организации сферы здравоохранения, но не оказывает существенного влияния на нарушение или прекращение критического бизнес-процесса.

53. ИС, ИТКС, АСУ, задействованная в реализации критического бизнес-процесса организации сферы здравоохранения, но не оказывающая существенного влияния на нарушение или прекращение критического бизнес-процесса (дублирующая автоматизация) считается объектом КИИ

организации сферы здравоохранения без присвоения категории значимости, установленной постановлением Правительства РФ от 08.02.2018 № 127.

54. ИС, ИТКС, АСУ, не задействованная в реализации критического бизнес-процесса, не является объектом КИИ организации сферы здравоохранения.

Методические рекомендации

по определению и категорированию объектов критической информационной инфраструктуры

топливно-энергетического комплекса

5. Выявление критических процессов в рамках видов деятельности, осуществляемых субъектом КИИ

Для каждого выявленного процесса должна быть проведена оценка критичности его нарушения с точки зрения возможных негативных социальных, политических, экономических, экологических последствий, последствий для обеспечения обороны страны, безопасности государства и правопорядка.

Необходимо отметить, что к критическим процессам следует относить только те процессы, которые исполняются в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ в областях (сферах), установленных п. 8 ст. 2 Федерального закона N 187-ФЗ, отраженные в уставе субъекта и внесенные в ЕГРЮЛ. В первую очередь должны рассматриваться процессы связанные с основной функциональной деятельностью, обеспечивающие получение прибыли предприятия.

Рекомендуется использовать перечень критериев значимости объектов и их значения из приложения 1 к Постановлению N 127. Соответственно, нужно определить для каждого рассматриваемого процесса, способно ли его нарушение повлечь последствия, определенные в Перечне.

Таким образом, отсекая на данном этапе процессы, нарушение которых не может привести к последствиям, соответствующим показателям значимости, автоматически отсекаются и системы (ИС, ИТКС, АСУ ТП), автоматизирующие данные процессы, так как их нарушение также не должно иметь значимых последствий.

Значения показателей критериев значимости оцениваются комиссионно на основании результатов интервью или иным способом, полученных в ходе обследования. По каждому показателю оценивается возможность наступления указанных видов последствий (возможно/невозможно). По результатам обработки предоставленной информации формируется перечень показателей критериев значимости, применимых для субъекта ТЭК.

Таким образом, критический процесс - процесс, для которого хотя бы по одному из оцениваемых показателей критериев значимости было сделано заключение о возможности соответствующего ущерба.

6. Определение объектов КИИ

Для каждого критического процесса формируется перечень ИС, ИТКС, АСУ ТП, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов.

Для каждого критичного процесса определяется перечень ИС, ИТКС, АСУ ТП, которые осуществляют одну из следующих функций:

- обработку информации, необходимой для критических процессов;
- управление критическим процессом;
- контроль или мониторинг критических процессов.

При формировании перечня членам комиссии рекомендуется:

- сделать запрос ответственным за ИС, ИТКС, АСУ ТП, ответственному за обеспечение безопасности объектов КИИ, ответственному по направлению информационных технологий или ответственному по направлению информационной безопасности с просьбой составить перечень ИС, ИТКС, АСУ ТП субъекта ТЭК;
- сделать запрос ответственному за выполнение процесса с просьбой указать перечень ИС, ИТКС, АСУ ТП, реализующих рассматривающие процессы. К запросу приложить сформированный общий перечень ИС, ИТКС, АСУ ТП;
- проанализировать итоговый перечень ИС, ИТКС, АСУ ТП на законность их владения

Методические рекомендации

по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи

6 Определение объектов критической информационной инфраструктуры

Определение объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и/или осуществляют управление, контроль или мониторинг критических процессов, осуществляется оператором связи на базе перечня типовых ИС, ИТКС и АСУ операторов связи, приведенного в приложении (см. Приложение В), исходя из перечня типовых критических процессов операторов связи (см. Таблица 2).

Группировка типовых ИС, ИТКС и АСУ операторов связи, а также сетей электросвязи представлена на рисунке ниже (см. Рисунок 4).

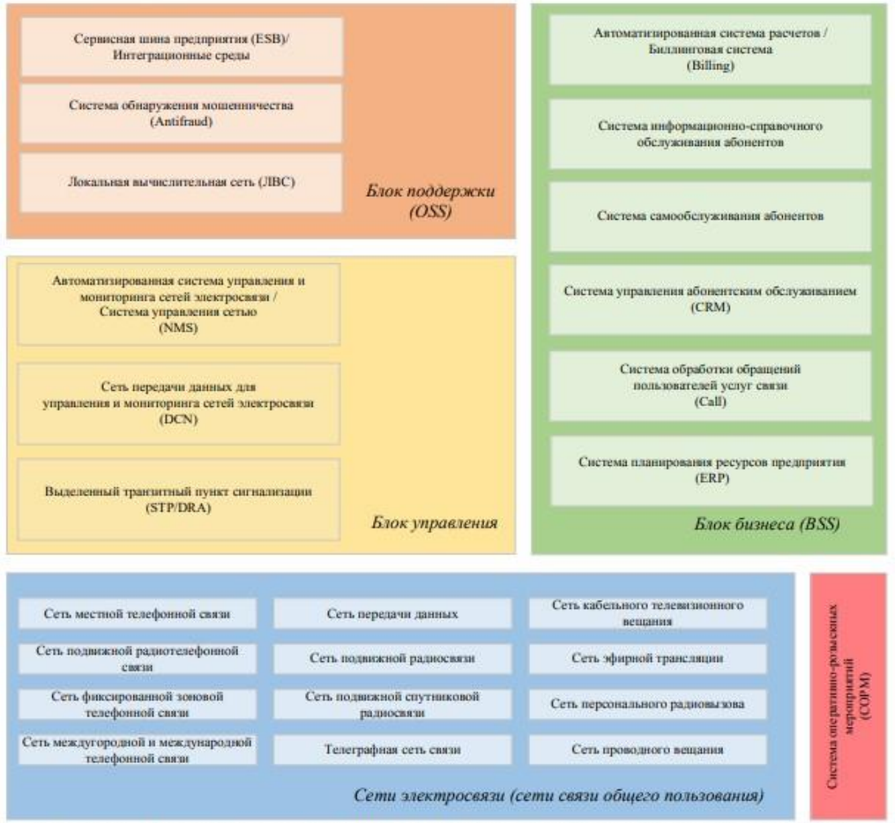
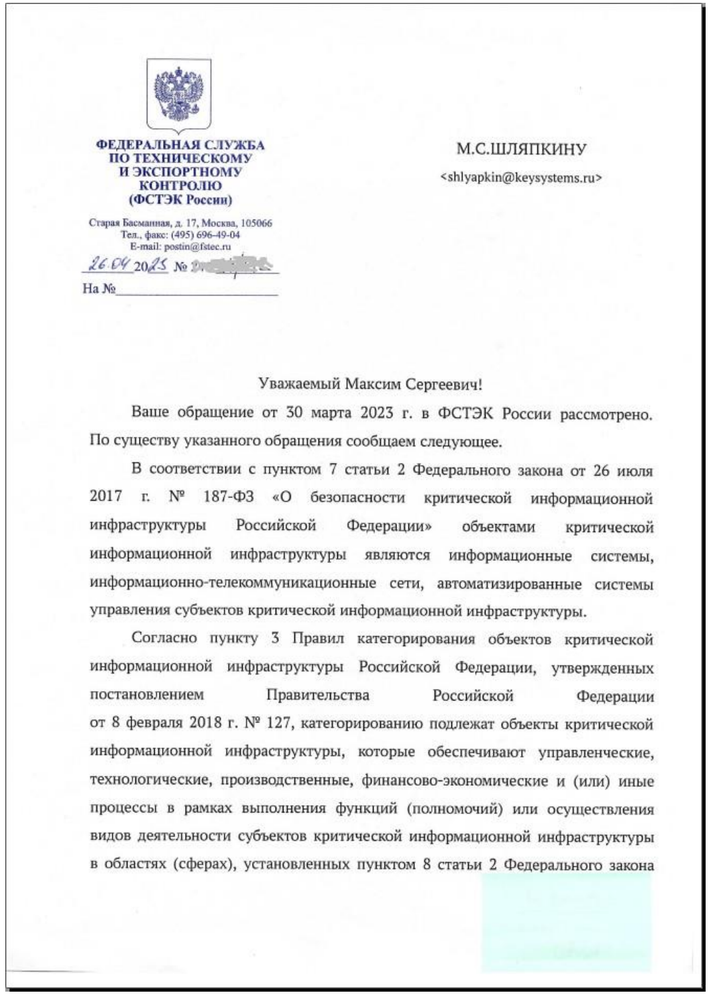


Рисунок 4 – Группировка типовых ИС, ИТКС, АСУ, сетей электросвязи операторов связи

Позиция ФСТЭК России



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)

Старая Басманная, д. 17, Москва, 105066
Тел., факс: (495) 696-49-04
E-mail: postin@fstec.ru

26.04.2023 № 2[redacted]

На №_____

М.С.ШЛЯПКИНУ

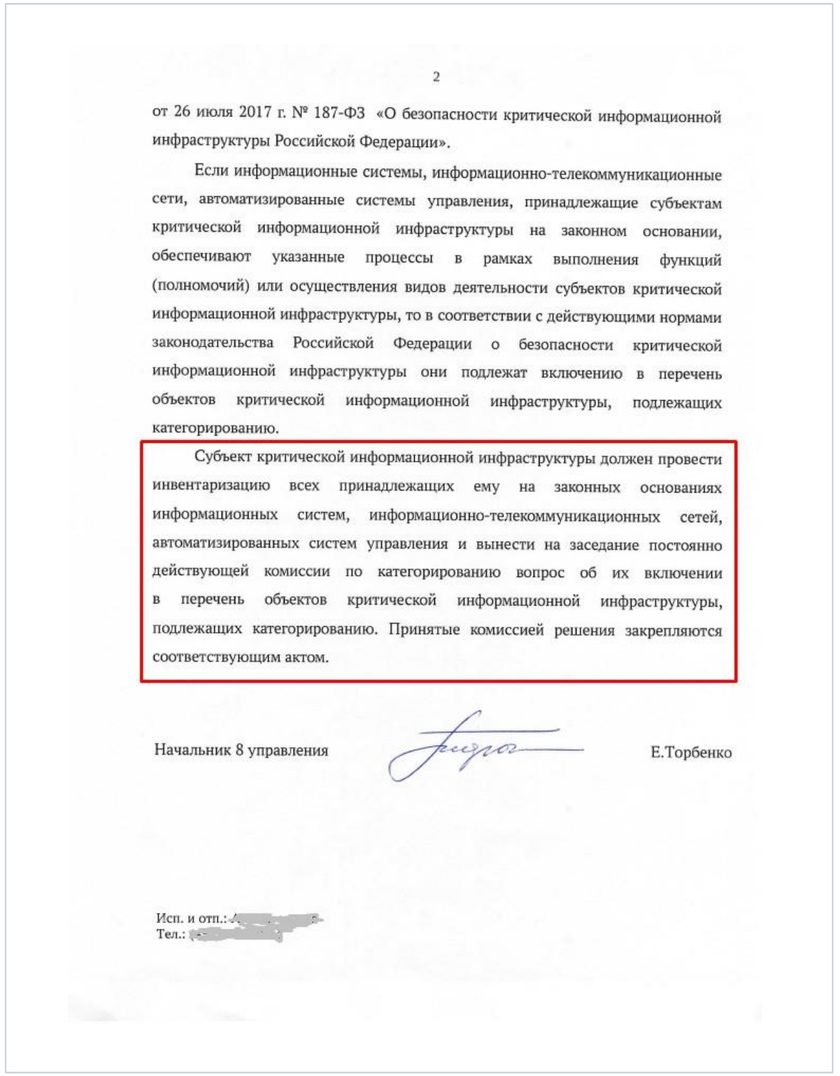
<shlyapkin@keysystems.ru>

Уважаемый Максим Сергеевич!

Ваше обращение от 30 марта 2023 г. в ФСТЭК России рассмотрено. По существу указанного обращения сообщаем следующее.

В соответствии с пунктом 7 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» объектами критической информационной инфраструктуры являются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Согласно пункту 3 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127, категорированию подлежат объекты критической информационной инфраструктуры, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона



2

от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Если информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, принадлежащие субъектам критической информационной инфраструктуры на законном основании, обеспечивают указанные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, то в соответствии с действующими нормами законодательства Российской Федерации о безопасности критической информационной инфраструктуры они подлежат включению в перечень объектов критической информационной инфраструктуры, подлежащих категорированию.

Субъект критической информационной инфраструктуры должен провести инвентаризацию всех принадлежащих ему на законных основаниях информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления и вынести на заседание постоянно действующей комиссии по категорированию вопрос об их включении в перечень объектов критической информационной инфраструктуры, подлежащих категорированию. Принятые комиссией решения закрепляются соответствующим актом.

Начальник 8 управления Е.Торбенко

Исп. и отп.: [redacted]
Тел.: [redacted]

Типовые перечни ОКИИ

Типовые перечни ОКИИ – это типы ИС/АСУ/ИТКС, которые могут иметься у субъекта КИИ с учетом его видов деятельности и которые должны быть включены в перечень объектов КИИ, подлежащих категорированию (при их наличии). Это НЕ перечень значимых объектов КИИ

Сферы, в которых на текущий момент (05.12.2023) утверждены типовые перечни:

- Транспорт - https://mintrans.gov.ru/documents/7/12506
- Энергетика - https://minenergo.gov.ru/opendata/7715847529-perechen-obektov-kii-2023
- ТЭК
- Наука
- Атомная промышленность
- Ракетно-космическая промышленность
- Банковская сфера и иные сферы финансового рынка

Алгоритм определения перечня объектов КИИ, подлежащих категорированию

Определение управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций или осуществления видов деятельности

Выявление критических процессов

Инвентаризация ИС/АСУ/ИТКС

Имеется типовой перечнь объектов КИИ в Вашей сфере деятельности?

Да

Сверка перечня ИС/АСУ/ИТКС с типовым перечнем ОКИИ, формирование перечня объектов КИИ, подлежащих категорированию с оформлением соответствующего акта

Категорирование ОКИИ

Нет

Формирования перечня ОКИИ, подлежащих категорированию с оформлением соответствующего акта

Процесс категорирования ОКИИ

Критерии залога успеха:

- **Полноценный состав** постоянно действующей комиссии по категорированию и ее **вовлеченность в процесс**
- **Подробное обоснование** полученных значений по каждому из рассчитываемых критериев значимости с приведением достоверных статистических данных, информации из регламентов проведения профилактических работ, отраслевых документов по функциональной безопасности и т.п.

Рекомендации:

- Рассматривайте **наихудшие сценарии** в результате проведения **целенаправленных компьютерных атак**
- Опирайтесь на декларации промышленной безопасности опасного производственного объекта, декларации безопасности гидротехнического сооружения, паспорты безопасности объекта топливно-энергетического комплекса (при наличии) и т.п., **но учитывайте последствия только в случае возникновения компьютерных инцидентов на ОКИИ**

Ответственность субъектов КИИ согласно КоАП

НПА	Статья	Тип нарушения	Наказание
		Административная ответственность	
КоАП РФ	13.12.1 (ч.1)	Нарушение требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов КИИ РФ, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ, если такие действия (бездействие) не содержат уголовно наказуемого деяния	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 50 000 до 100 000 рублей.
	13.12.1 (ч.2)	Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ, установленного федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.
	13.12.1 (ч.3)	Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными организациями, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты	• для должностных лиц – штраф от 20 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.
	19.7.15 (ч.1)	Непредставление или нарушение сроков представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, сведений о результатах присвоения объекту КИИ РФ одной из категорий значимости, предусмотренных законодательством в области обеспечения безопасности КИИ РФ, либо об отсутствии необходимости присвоения ему одной из таких категорий либо представление недостоверных сведений	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • за повторное нарушение – штраф от 10 000 до 50 000 рублей (ч.3 ст. 19.7.15); • для юридических лиц – штраф от 50 000 до 100 000 рублей; • за повторное нарушение – штраф от 100 000 до 200 000 рублей (ч.3 ст. 19.7.15).
	19.7.15 (ч.2)	Непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ информации, предусмотренной законодательством в области обеспечения безопасности КИИ РФ, за исключением случаев, предусмотренных частью 2 статьи 13.12.1 КоАП	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.

Основные шаги субъектов КИИ в части выполнения требований законодательства РФ

1. Провести категорирование объектов КИИ
2. Отправить результаты категорирования объектов КИИ во ФСТЭК России.
3. **Разработать техническое задание на создание системы информационной безопасности значимых объектов КИИ**.
4. **Провести анализ угроз безопасности информации и разработать модели угроз безопасности информации значимых объектов КИИ**.
5. **Провести проектирование системы информационной безопасности значимых объектов КИИ.**
6. **Разработать рабочую (эксплуатационную) документацию на систему информационной безопасности значимых объектов КИИ**.
7. Закупить, установить и настроить средства защиты информации для обеспечения безопасности значимых объектов КИИ.
8. Разработать организационно-распорядительную документацию о правилах и процедурах обеспечения безопасности значимых объектов КИИ.
9. Провести предварительные испытания системы безопасности значимых объектов КИИ.
10. Провести анализ уязвимостей значимых объектов КИИ и принять меры по их устранению.
11. Провести приемочные испытания значимых объектов КИИ и системы информационной безопасности.
12. Организовать взаимодействие с ГосСОПКА.

- **С 1 сентября 2024 г. не допускается** использование субъектами КИИ РФ … программно-аппаратных комплексов, приобретённых … с 1 сентября 2024 г. и не являющихся доверенными программно-аппаратными комплексами, за исключением случаев отсутствия произведенных в РФ доверенных программно-аппаратных комплексов, являющихся аналогами…

- Переход субъектов КИИ РФ на преимущественное применение доверенных ПАК на принадлежащих им значимых объектах КИИ РФ **должен быть завершен до 1 января 2030 года.**

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 14 ноября 2023 г. № 1912

МОСКВА

О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации

Во исполнение пункта 2 Указа Президента Российской Федерации от 30 марта 2022 г. № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации" Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые Правила перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации.

2. Установить, что:

переход субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации осуществляется до 1 января 2030 г. в соответствии с Правилами, утвержденными настоящим постановлением;

с 1 сентября 2024 г. не допускается использование субъектами критической информационной инфраструктуры Российской Федерации

О КОМПАНИИ

Компания QTECH (КЬЮТЭК) основана в 2006 году как разработчик телекоммуникационных решений.

Центральный офис компании расположен в Москве. В крупнейших городах России работают филиалы. QTECH имеет свои R&D центры в Москве и Рязани.

ЛИДЕР ОТРАСЛИ 2022

Sk Участник

8 офисов

3 R&D центра

Центр Технической поддержки

Складские и производственные мощности

ПРОИЗВОДСТВО

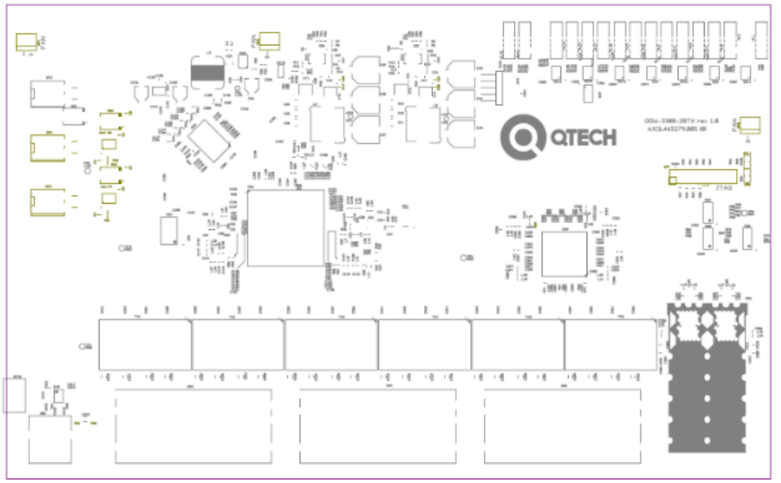
РАЗРАБОТКА СХЕМОТЕХНИКИ

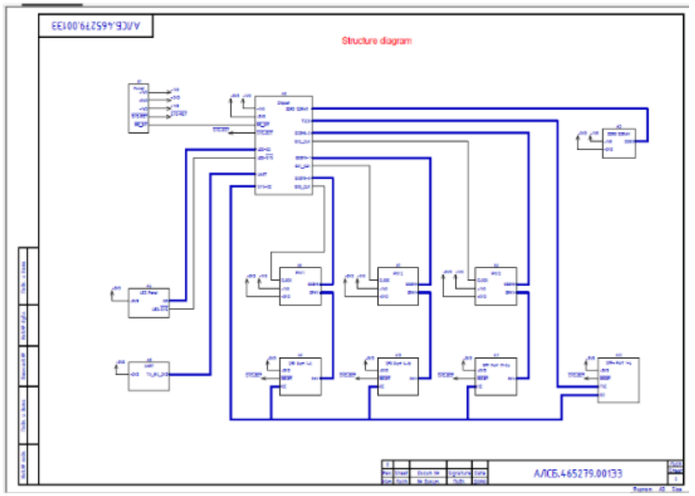
ЧИПСЕТЫ

ПАМЯТЬ FLASH, RAM

БЛОКИ ПИТАНИЯ

Максимальное использование отечественных комплектующих





R&D ЦЕНТРЫ QTECH

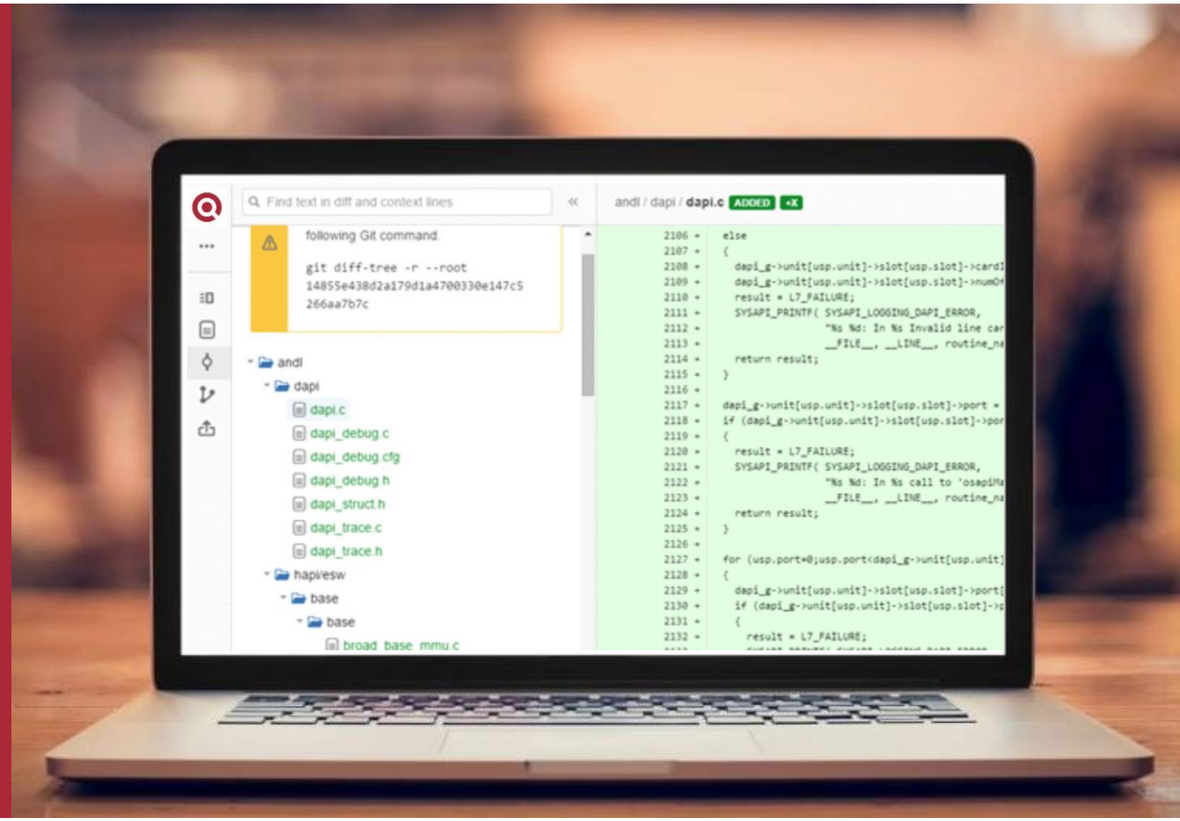
- г. Москва
- г. Рязань

ПРОИЗВОДСТВО QTECH

- г. Санкт-Петербург
- г. Пермь
- г. Кострома
- г. Арзамас

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

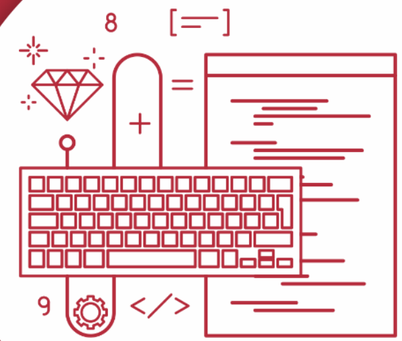
- Сформирована команда разработчиков ПО, полностью закрывающая технологические потребности разработки оборудования QTECH.
- Программисты работают в тесной связи с разработчиками аппаратных решений и технической поддержкой чипмейкеров (Marvell, Realtek, Baikal, Элвис и другие).
- Программные модули разрабатываются программистами компании.
- Обеспечивается полный контроль жизненного цикла ПО и возможность непрерывных улучшений и добавления функционала.



ПРЕИМУЩЕСТВА СОБСТВЕННОЙ РАЗРАБОТКИ

СКОРОСТЬ РАЗРАБОТКИ / ДОРАБОТКИ

цикл разработки программного обеспечения занимает меньше времени



ГИБКОСТЬ

дорабатываем программное обеспечение под меняющиеся нужды заказчика

ИМПОРТОЗАМЕЩЕНИЕ

QTECH – поставщик проекта «Цифровая Экономика»

Минцифры России

Программные решения QTECH внесены **в Единый реестр российских программ для электронных вычислительных машин и баз данных**

МИНПРОМТОРГ РОССИИ

Оборудование QTECH внесено в **Единый реестр российской радиоэлектронной продукции и Реестр промышленной продукции, произведенной на территории РФ**

Резидент Консорциума АНО «Телекоммуникационные технологии» (АНО ТТ) как российский разработчик телекоммуникационного и IT-оборудования

МВД

Оборудование QTECH получило сертификат транспортной безопасности **№ 969**

QTECH – член Торгово-промышленной палаты Российской Федерации

ПОРТРЕТ ЗАКАЗЧИКА

Заказчик корпоративного уровня

01 От малых до больших размеров

02 Имеющий собственную ИТ инфраструктуру

03 Имеющих как локальное, так и географически разнесённое положение

Потребность в построении новой ИТ инфраструктуры с нуля, модернизация существующей ИТ инфраструктуры, импортозамещение, расширение бизнеса, укрупнение компании и т.д.

НАШИ КЛИЕНТЫ

QTECH
МИР ДОСТУПНЕЕ

ОПЕРАТОРЫ СВЯЗИ И ИНТЕРНЕТ-ПРОВАЙДЕРЫ

ГОСУДАРСТВЕННЫЕ СТРУКТУРЫ

ПРОИЗВОДСТВЕННЫЕ ПРЕДПРИЯТИЯ

КОММЕРЧЕСКИЕ КОМПАНИИ

СТРОИТЕЛЬНО-МОНТАЖНЫЕ ОРГАНИЗАЦИИ

ДЕВЕЛОПЕРЫ

УПРАВЛЯЮЩИЕ КОМПАНИИ

ИНТЕГРАТОРЫ

Генеральная прокуратура РФ

ФСИН

Министерство финансов РФ

МВД

Администрации городов РФ

Федеральная налоговая служба

Фонд социального страхования

Банк России

ГАЗПРОМ

ТРАНСНЕФТЬ

УГМК UMMC

ЯМАЛ СПГ

АТС Смольного

МАГНИТ

Московский Метрополитен

ФСК ЕЭС

TATNEFT

Ростелеком

МТС

билайн

МегаФон

ЭР-ТЕЛЕКОМ

ТТК

Bashtel

уфанет
друзья всегда с тобой

КОМПЛЕКСНЫЕ РЕШЕНИЯ НА РОССИЙСКИХ ПРОДУКТАХ QTECH

QTECH
МИР ДОСТУПНЕЕ

Серверы и СХД

- 1 и 2 контроллерные СХД (Hybrid All Flash)
- 1 и 2 процессорные на базе Intel

Wi-Fi

- Точки доступа 5 и 6 поколений
- Контроллеры с поддержкой до 20 000 пользователей

Инженерные системы

- Телекоммуникационные шкафы

IP-телефония

- IP-телефонные аппараты
- от простых до директорских

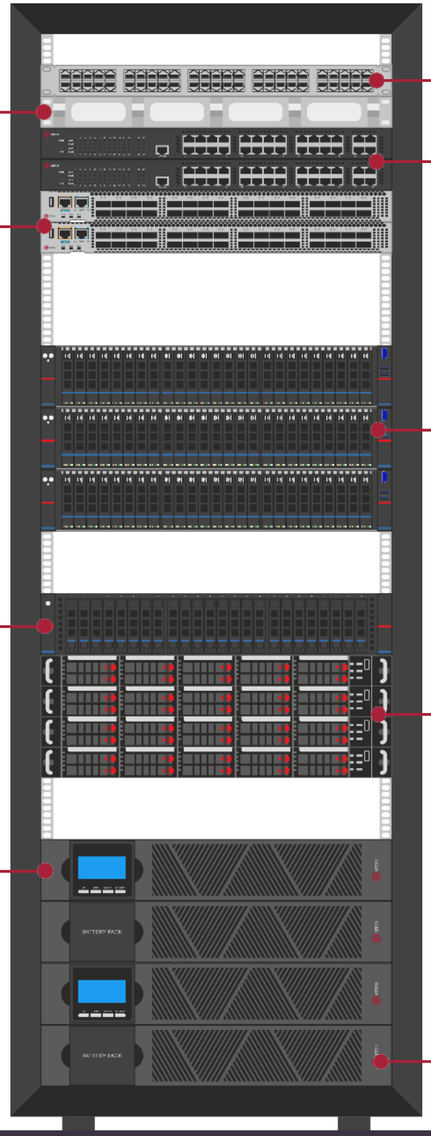
Сетевое оборудование

- Доступ: 1G / 2.5G / 10G
- Агрегация: 1G / 10G
- Ядро: 10G / 100G
- ЦОД: 25G / 100G
- Сервисные маршрутизаторы

Видеонаблюдение

- IP-камеры до 8 мП
- Видеорегистраторы

КОМПЛЕКСНЫЙ ПОДХОД



Маршрутизатор QTECH QSR

Стек коммутаторов доступа QTECH QSW

Видеорегистратор QTECH QVC-NVR

Источники бесперебойного питания QTECH QPS

Коммутатор ядра QTECH QSW

Кластер коммутаторов агрегации QTECH QSW

Серверы QTECH QSRV с контроллером БЛВС QTECH QWC и кластерной системой АТС QTECH QPBX-QX

Система хранения данных QTECH QSRV

Шкаф напольный QTECH RECQ

2

ГАРАНТИЙНАЯ И ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

QTECH
МИР ДОСТУПНЕЕ

Гарантийная и техническая поддержка
до 5-и лет

	БАЗОВЫЙ	РАСШИРЕННЫЙ*	ПРЕМИУМ*
Режим поддержки	8/5	8/5	24/7
Время реакции	До 8 часов	До 4 часов	До 2 часов
Время реакции на критический инцидент	До 2 часов	До 1 часа	До 30 минут
Бесплатная консультация специалиста	✓	✓	✓
Помощь в устранении инцидента	Удаленно	Выезд инженера**	Выезд инженера**
Срок замены неисправного оборудования	На гарантии 2-30 дней	NBD***	NBD***

*Тариф «Расширенный» и «Премиум» можно приобрести только на коммутаторы, маршрутизаторы, серверы, СХД и Wi-Fi оборудование.

Выезд инженера - Услуга, которая приобретается только для тарифных пакетов **«Расширенный» (выезд в пределах Москвы) и **«Премиум»** (выезд по всей территории РФ) и оплачивается отдельно Заказчиком.

***NBD - отправка оборудования на подмену на следующий рабочий день с момента подтверждения неисправности инженером QTECH

3 CISCO LIKE CLI ИНТЕРФЕЙС

ИНЖЕНЕРАМ НЕ ТРЕБУЕТСЯ ПЕРЕУЧИВАТЬСЯ:
синтаксис команд оборудования QTECH полностью аналогичен оборудованию Cisco

Пример CLI (command-line interface) коммутаторов QTECH:

4

ОБУЧЕНИЕ

УЧЕБНЫЙ КУРС - Сетевые технологии QTECH

QTECH
МИР ДОСТУПНЕЕ

МИКРОТЕСТ®
УЧЕБНЫЙ ЦЕНТР

Программа курса разработана Учебным центром «Микротест» в соответствии с профессиональным стандартом "Специалист по администрированию сетевых устройств информационно-коммуникационных систем".

Кому полезен курс:

- Инженерам сопровождения и технической поддержки
- Системным администраторам
- Специалистам технических и инженерных служб

Базовый уровень – QTECH Network Basic — Подробнее >>>

Профессиональный уровень – Network Professional Fast Track — Подробнее >>>

По окончании курса выдается удостоверение о повышении квалификации, а также сертификат QTECH.

Обучение проводит УЦ «Микротест»

СОВМЕСТИМОСТЬ

QTECH
МИР ДОСТУПНЕЕ

Windows Server

redhat LINUX

vmware ESXi
vmware vSphere

base alt

KVM

PROXMOX

РЕДСОФТ

КОД безопасности

БРЕСТ
СКАЛА-Р

ASTRA LINUX®
special edition

РОСА

ROSA

Оборудование QTECH использует общепринятые протоколы и совместимо с оборудованием других производителей. Мы анализируем потребности рынка и учитываем эти потребности в наших будущих разработках, тем самым повышая качество, надежность и импортонезависимость оборудования QTECH.

МОДЕЛЬНЫЙ РЯД СЕРВЕРОВ QTECH
Конфигурирование

	Сервер 4U QSRV-462402; 24*3.5 + 2*2,5 SAS + 2*2.5 U.2 HS HDD; CPU 2*Xeon Gold 5218R 20core 2,0GHz; 12*32GB RDIMM DDR4 2933; Trimode 2GB Cache Raid 0,1,5,6,50,60, 10; SSD 2*480GB SATA + 2*960GB SSD U.2 dwpd 1 HS; HDD 24*8TB 7.2k SAS HS; 2*1GbE LAN; 2*10GbE SFP+ LAN OCP; 3*x8 PCI-e; 2*800W AC (1+1); IPMI; Rails; Гарантия 3 года.	**1**
QSRV-462402	Сервер 4U QSRV-462402 24*3,5 HDD; 2*Intel SL (LGA 3647 max 205W tdp); 24*DDR4; Software Raid 0,1,5 & 10; PCI-E 4X 2*M.2; 2*550W(1+1); 2*1GbE LAN; 3*X8 PCI-E; IPMI; Rails	1
08RPSU	2*800W	1
G5218R	Gold 5218R	2
32RD29	32GB RDIMM ECC 2933	12
210OCP	2*10G OCP 3.0	1
94XX16I2GR	Trimode 94xx 2GB Raid 16i	1
2,5U2bay	2*2,5" NVMe rear bay	1
2,5SASbay	2*2,5" SAS rear bay	1
960SU2d1	960GB SSD U.2 dwpd 1	2
480SSATAd1	480GB SSD SATA dwpd 1	2
8HD7SAS3,5	8TB 7.2k SAS 3,5	24

Доступ к конфигуратору предоставляется по запросу.
Внешний адрес - http://srvcfg.qtech.ru:8080/

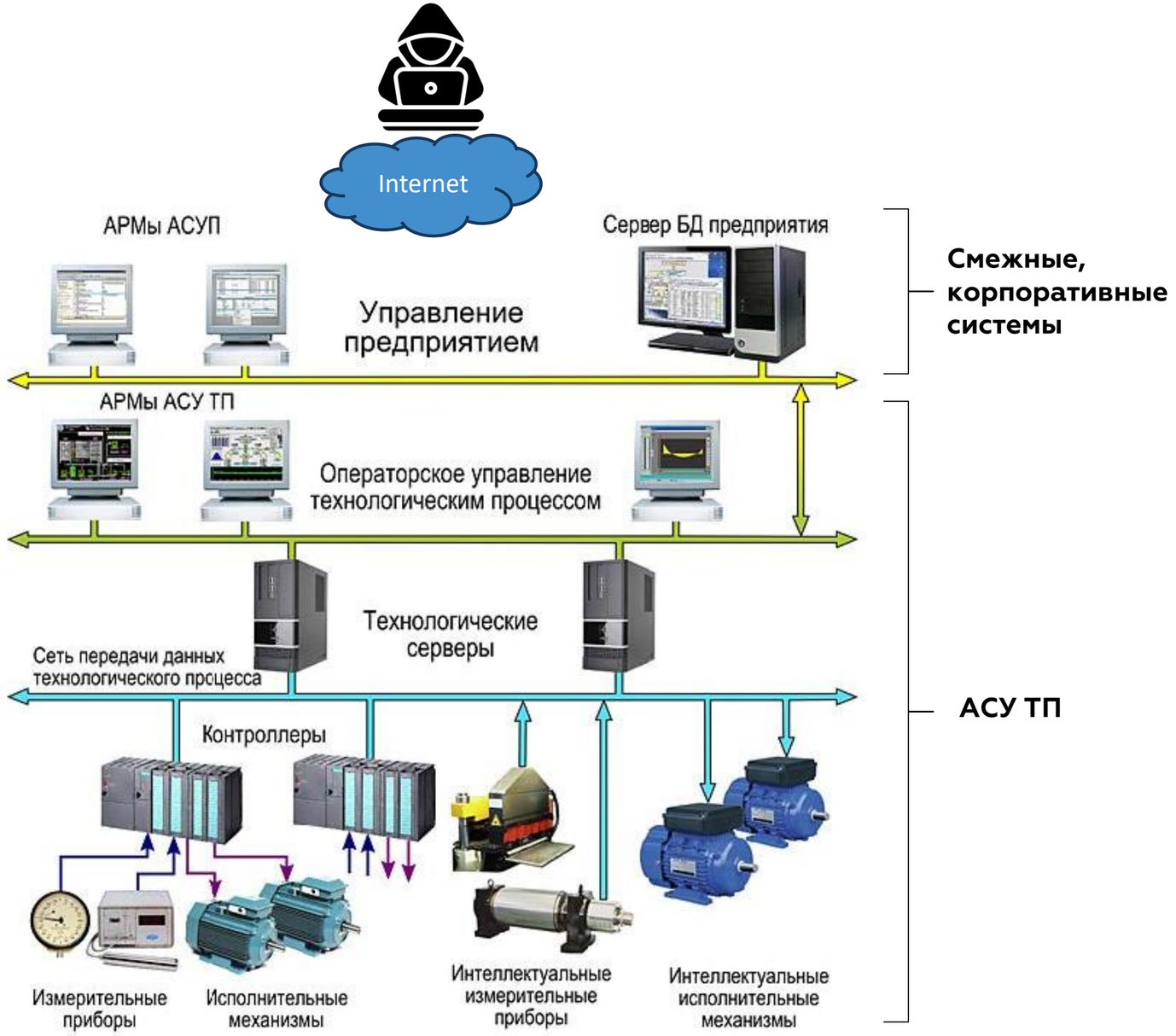
Проектирование системы защиты – лицензируемый вид деятельности

Согласно ПП РФ №79 от 03.02.2012 «О лицензировании деятельности по ТЗКИ»:

При осуществлении лицензируемого вида деятельности лицензированию подлежат:

a) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам [...];
b) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
c) услуги по мониторингу информационной безопасности средств и систем информатизации;
d) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации [...];
e) работы и услуги по проектированию в защищенном исполнении [...];
f) услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации [...].

Что защищать?



Подготовка к внедрению системы защиты

Мероприятие	Рекомендации
Подготовка помещений для размещения СрЗИ	• выделите место (помещение) под размещение шкафа для СрЗИ; • убедитесь, что помещение охлаждаемое; • шкафы для размещения СрЗИ должны быть оборудованы охранной сигнализацией; • помещения, для размещения оборудования должны быть оснащены системой видеонаблюдения и контроля управления доступом; • учитывайте требования производителей СрЗИ
Подготовка локально-вычислительной сети	• проведите инвентаризацию ЛВС: выясните модели коммутаторов, их расположение, пропускную способность, наличие возможности настройки зеркалирования траффика (SPAN-порты);
Тестирование СрЗИ	• проверьте СрЗИ на совместимость с компонентами ОКИИ – проведите пилотирование СЗИ; • убедитесь, что СрЗИ не будут оказывать воздействие на технологическую сеть
Период внедрения системы защиты	• планируйте внедрение системы защиты во время плановой модернизации ОКИИ
Импортозамещение	• планируйте мероприятия по переходу на отечественное ПО и оборудование • проверяйте отечественные решения на совместимость с инфраструктурой ОКИИ
ГосСОПКА	• для полноценного мониторинга ИБ подключайте к SIEM как можно больше источников событий • в случае отсутствия возможности качественно осуществлять мониторинг ИБ, подключайтесь к корпоративным центрам мониторинга
Выполнение работ по созданию системы ИБ	• в случае ограниченности бюджета, планируйте поэтапное выполнение работ по ИБ

Организационные меры в отношении персонала субъекта КИИ

ЗАПРЕТИТЬ:

- использовать посторонние USB-накопители на АРМ промышленной сети;
- заходить в личную почту через АРМ промышленной сети;
- загружать и устанавливать стороннее ПО на АРМ промышленной сети;
- передавать конфиденциальную информацию (файлы) через внешние облачные сервисы;
- скачивать файлы из внешних источников на АРМ промышленной сети;
- пользоваться социальными сетями на рабочем месте;
- развертывать дополнительные Wi-Fi сети на территории промышленного объекта;
- заряжать лишние устройства через АРМ и серверы промышленной сети

Рекомендации от регулятора

Защита от атак «отказ в обслуживании»

Исх. № 240/84/2582 от 30 сентября 2022 г.

✓ **Канальный уровень:**

- Заключить договор с провайдером на предоставление соответствующей услуги

✓ **Прикладной уровень:**

- исключить неиспользуемые сетевые интерфейсы и протоколы;
- не размещать в одной сети общедоступные ресурсы и ресурсы, обеспечивающие выход в «Интернет»;
- размещать общедоступные ресурсы во внешнем облаке провайдера
- исключить прямое подключение ЗО КИИ к ССОП;
- резервирование каналов обмена информации ЗО КИИ с ССОП
- использовать серверное оборудование, способное выдержать большие нагрузки при обработке TLS-трафика прикладных запросов;
- настроить межсетевые экраны в части сокращения таймаутов
- не размещать в общедоступных ресурсах сервисы по UDP-протоколу или осуществить их перевод на TCP-протокол;
- вывести сервисы с UDP-протоколом в отдельную подсеть;
- обеспечить защиту от атак на таблицу состояний и ограничения по количеству одновременных соединений с одного IP-адреса;
- организовать фильтрацию трафика на прикладном уровне
- проводить регулярную инвентаризацию общедоступного IP-адресного пространства, с целью своевременного реагирования на подмену или компрометацию

9

Информационное сообщение ФСТЭК России о мерах по повышению защищенности информационной инфраструктуры:

https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-24-marta-2022-g-n-240-22-1549

ТГ-КАНАЛ: Листок бюрократической защиты информации

- Нормативно-новостной канал по теме организационной и правовой защиты информации в Российской Федерации

Система нормативных правовых актов, методических и информационных документов в области обеспечения безопасности КИИ

Куар-код на актуальную подборку законодательных документов по КИИ

Услуги КСБ-СОФТ

Компания КСБ-СОФТ оказывает полный комплекс услуг по защите объектов КИИ

Мы поможем Вам защитить данные и выполнить требования НПА

Безопасность объектов КИИ

Выявление и категорирование объектов КИИ, разработка и внедрение комплексного решения по обеспечению безопасности значимых объектов КИИ, организация взаимодействия с центром ГосСОПКА, анализ уязвимостей и пентест

Импортозамещение

Решение задач импортозамещения в соответствии со стратегией развития информационного общества в Российской Федерации

SOCRAT - центр мониторинга и реагирования на инциденты информационной безопасности

Мониторинг и предотвращение атак на начальных стадиях, либо выявление следов проникновения

https://rutube.ru/video/8048df2267bf671cd042799a7da6a088/?r=wd

ПК АльфаДок. Автоматизация процессов по защите информации

альфа|док

- Разработка и актуализация документации, журналов
- Учет защищаемых ресурсов и средств защиты информации
- Моделирование угроз безопасности и определение мер по защите информации
- Оценка защищенности систем, анализ уязвимостей
- Категорирование объектов КИИ с разработкой документации в соответствии с приказом ФСТЭК России № 239
- Планирование деятельности, оценка готовности к проверкам
- Учет и реагирование на инциденты информационной безопасности

Специальное предложение

Эскизное проектирование подсистемы
информационной безопасности для объекта КИИ
(формат - дистанционный)

+ первым 5-ти записавшимся на проект – предпроектный аудит бесплатно!

Работайте с нами!

https://ksb-soft.ru/

428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9

8 800 3333-872

info@ksb-soft.ru

Телеграм-канал
«Мнение интегратора»