Анализ нормативной базы в области информационной безопасности и доверенные программно-аппаратные комплексы

7 февраля 2024 года

Актуальность проблемы обеспечения информационной безопасности

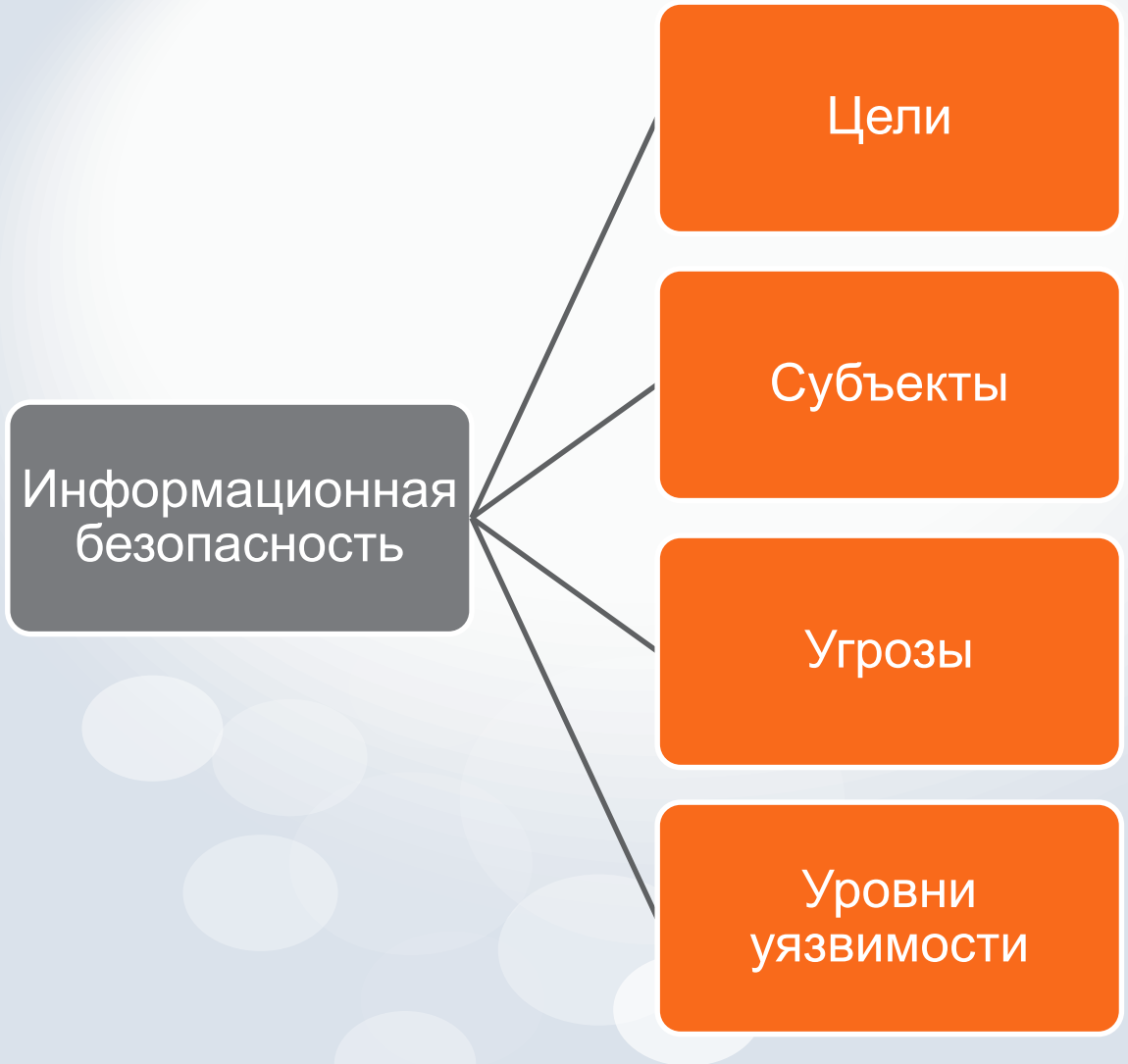
Актуальность проблемы обеспечения информационной безопасности обусловлена следующими факторами:

- ✓ быстрые темпы роста количества различных электронных устройств, применяемых в самых разных сферах деятельности, и, как следствие, резкое расширение круга пользователей, имеющих непосредственный доступ к сетям и информационным ресурсам;
- ✓ резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
- ✓ бурное развитие аппаратно-программных средств и технологий, не соответствующих современным требованиям безопасности;
- ✓ несоответствие развития средств обработки информации и проработки теории информационной безопасности, разработки международных стандартов и правовых норм, обеспечивающих необходимый уровень защиты информации;
- ✓ повсеместное распространение сетевых технологий, создание единого информационно-коммуникационного мирового пространства на базе Интернет (например, «Интернет вещей (IoT)»), которая по своей идеологии не обеспечивает достаточного уровня информационной безопасности.
- ✓ высокий ежегодный рост количества компьютерных преступлений в мире и России и ущерба, причиняемого такими преступлениями.

Обеспечение ИБ КИИ Российской Федерации – важная составляющая государственного суверенитета

- ✓ Создание специализированных подразделений в вооруженных силах государств НАТО численностью в десятки тысяч человек, основная задача которых заключается в выведении из строя инфраструктуры жизнеобеспечения и банковской сферы государств - «противников» путем кибератак;
- ✓ Прямые угрозы первых лиц США о возможных кибератаках на инфраструктуру Российской Федерации;
- ✓ Геополитическая ситуация (внешний фактор), что привело к ограничению ввоза в РФ продукции высокотехнологичных отраслей и технологий двойного назначения;
- ✓ Расширение внутренних ограничений (внутренний фактор) на отрасли экономики (предприятия) закономерно и вынужденно попадающие под ограничение использования импортной микроэлектроники и программного обеспечения;
- ✓ Возникновение новых рисков увеличения вероятности кибератак на критическую информационную инфраструктуру (КИИ) РФ, последствия которых сопоставимы, например, с аварией на Саяно-Шушенской ГЭС, что заставляет учитывать при создании объектов КИИ вопросы ИБ как одну из основных частей, а не как сторонний элемент, который можно будет добавить потом;
- ✓ Технологическая готовность и развитие отечественных аппаратно-программных платформ, что создает благоприятные условия к снижению зависимости от импорта технологий, созданию действительно отечественных (не локализованных) аналогов интеллектуального оборудования различного назначения.

Структурная модель ИБ (с точки зрения правовых отношений)

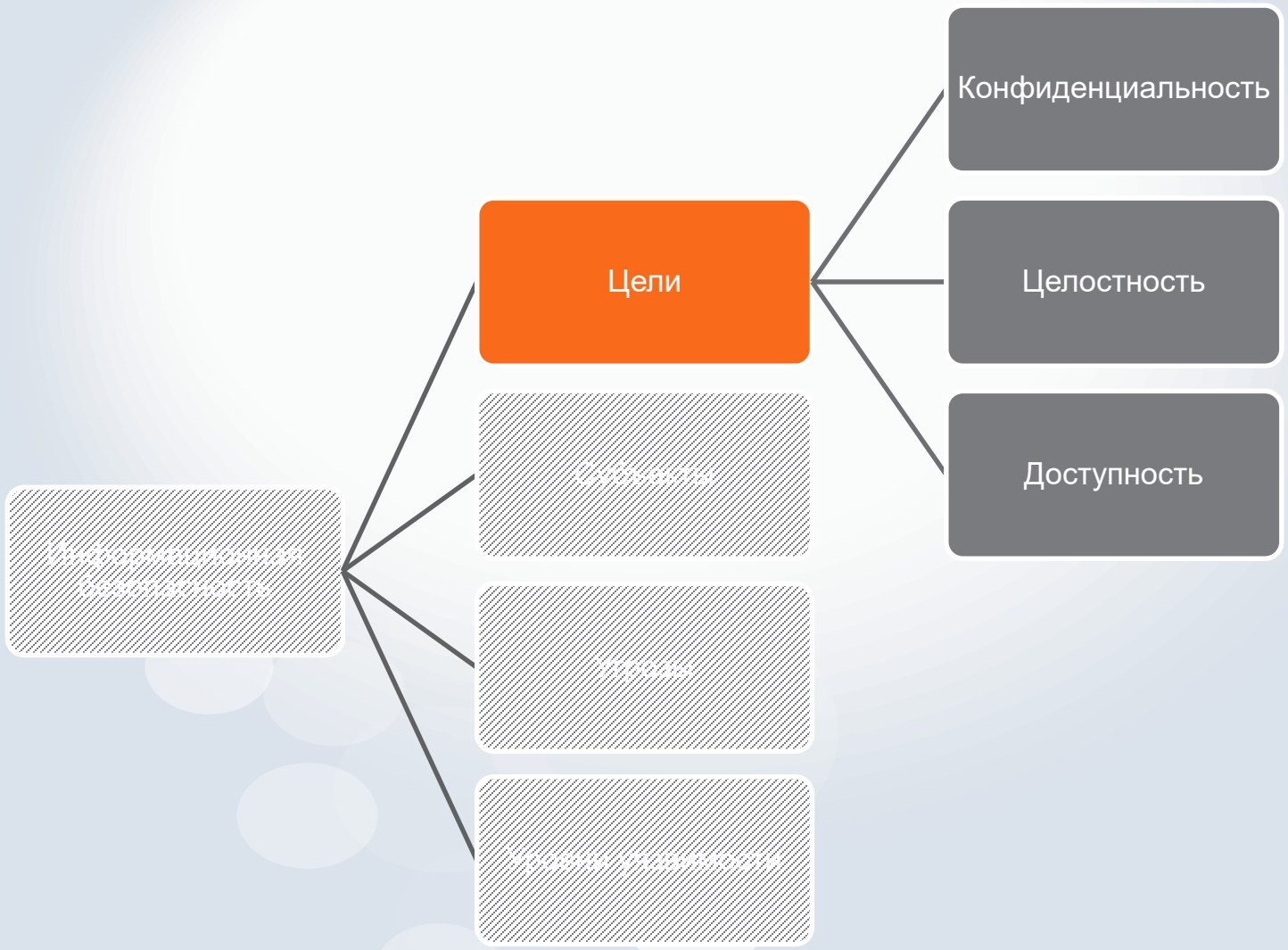


С точки зрения правовых отношений структурную модель информационной безопасности компьютерных систем можно представить в виде схемы, показанной на рисунке.

Основными структурными элементами информационной безопасности компьютерных систем в данной модели являются:

1. Цели защиты информации.
2. Субъекты, участвующие в процессах информационного обмена.
3. Угрозы безопасности информационных систем.
4. Уровни уязвимости информации и информационной инфраструктуры.

Структурная модель ИБ (с точки зрения правовых отношений). Цели.



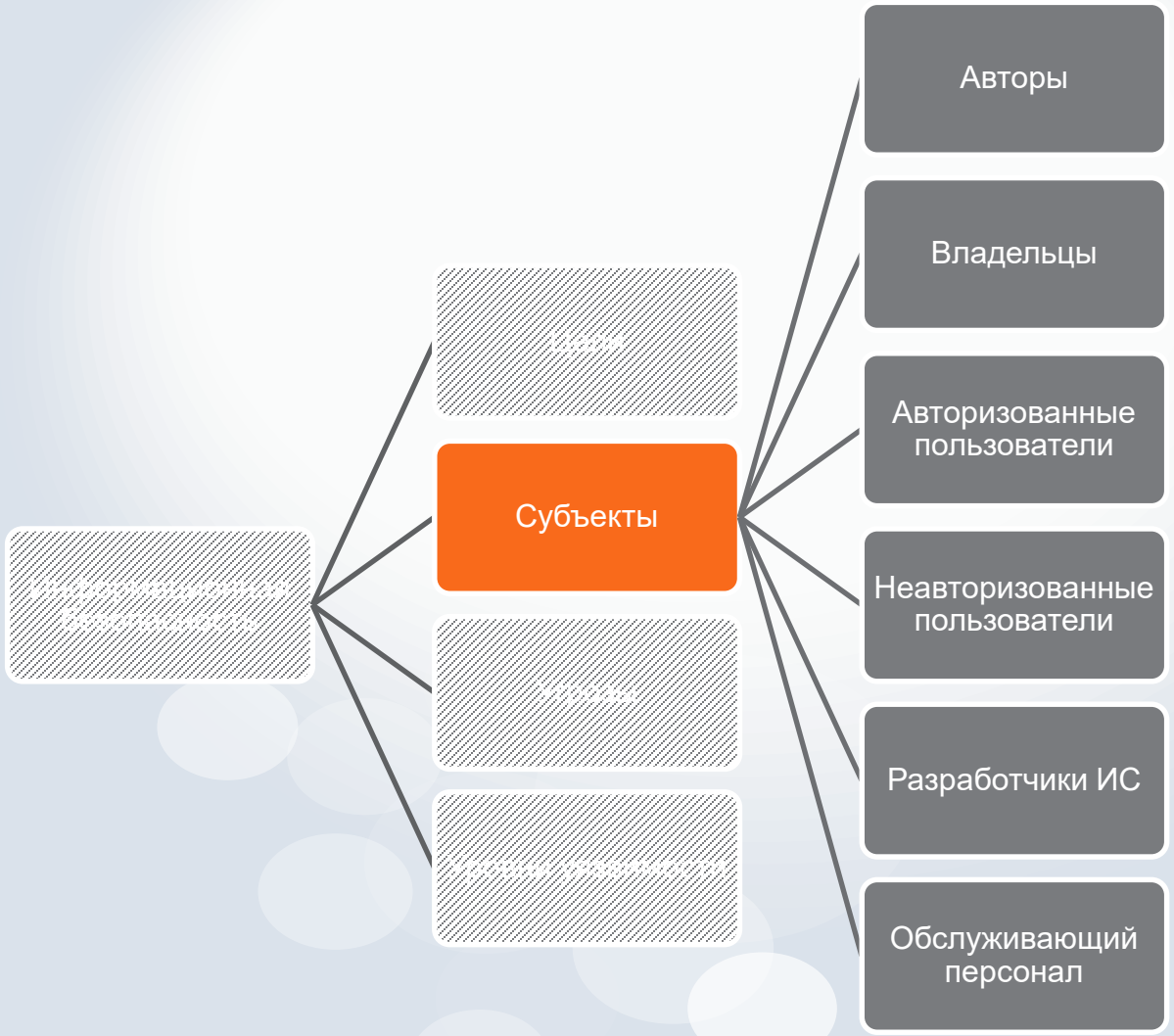
Обеспечение безопасности состоит в достижении 3-х взаимосвязанных целей — конфиденциальность, целостность и доступность.

Обеспечение конфиденциальности состоит в защите информации в процессе ее создания, хранения, обработки и обмена по каналам связи от ознакомления с ней лицами, не имеющими права доступа. Кроме того, авторизованные пользователи системы должны иметь доступ к информации в соответствии с установленными правами.

Обеспечение целостности состоит в защите от преднамеренного или непреднамеренного изменения информации и алгоритмов ее обработки лицами, не имеющими на то права.

Обеспечение доступности состоит в предоставлении авторизованным пользователям всей имеющейся в системе информации в соответствии с установленными правами доступа.

Структурная модель ИБ (с точки зрения правовых отношений). Субъекты.



Основными субъектами в информационных процессах являются: **авторы** (собственники) информационных ресурсов, владельцы информации, авторизованные пользователи, неавторизованные пользователи, разработчики информационной системы, обслуживающий персонал, обеспечивающий работоспособность программно-технических средств и средств защиты, а также персонал, занимающийся наполнением системы информацией.

Владельцы информации обязаны построить систему защиты, которая должна обеспечивать соблюдение авторских прав собственникам информации и предоставлять доступ к информации только **авторизованным пользователям** в соответствии с их правами.

Неавторизованные пользователи стремятся получить несанкционированный доступ к информационной системе. Кроме того, возможны каналы утечки информации, заложенные **разработчиками информационной системы** и известные только им (недокументированные возможности).

Персонал, занимающийся сопровождением программно-технических средств, администрированием сети, обеспечением защиты и информационным наполнением, также представляет определенную угрозу несанкционированных утечек информации, а потому является важным субъектом информационных процессов. Как правило, обслуживающий персонал не всегда имеет полноправный доступ к информации в системе, но имеет практически неограниченный доступ к аппаратно-программным средствам и телекоммуникациям, обеспечивающим функционирование всей информационной системы.

Структурная модель ИБ (с точки зрения правовых отношений). Угрозы.

Под угрозой безопасности информационных систем понимается потенциально возможное действие, событие или процесс, которые посредством воздействия на информацию и другие компоненты системы могут нанести ущерб интересам субъектов. Прежде всего, по результатам воздействия угрозы бывают пассивные и активные.

Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов сети, не оказывая при этом влияния на ее функционирование и информационное наполнение. **Активные угрозы** имеют целью нарушение нормального функционирования ИС путем целенаправленного воздействия на ее компоненты. Активные угрозы безопасности могут быть разделены на естественные и искусственные. **Естественные угрозы** — это угрозы, вызванные воздействием на информационные системы объективных физических процессов или стихийных природных явлений, не зависящих от человека. **Искусственные угрозы** вызваны действиями человека (антропогенные) и подразделяются на непреднамеренные (случайные) и преднамеренные. Данная группа угроз самая обширная. Она представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия этим угрозам управляемы и в основном зависят от организаторов защиты информации. **Непреднамеренные угрозы** связаны с людьми, непосредственно работающими с компьютерной системой (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, но без злого умысла). **Преднамеренные искусственные угрозы** делятся на **внутренние** (со стороны персонала организации) и **внешние** (от посторонних лиц и организаций). В свою очередь, внешние угрозы подразделяются на **локальные** (проникновение посторонних лиц в учреждение и доступ их к системе) и **удаленные** (незаконный доступ к системе через глобальные сети).

Структурная модель ИБ (с точки зрения правовых отношений). Уровни уязвимости.

Уязвимость информационных систем можно классифицировать по уровням: физический, технологический, логический, человеческий, законодательный, организационный.

Физический уровень определяет, насколько эффективно защищены элементы, образующие техническую часть информационной системы: сервера, рабочие станции, периферийные устройства, коммуникационное оборудование и линии связи.

Технологический уровень отражает эффективность защиты аппаратно-программных процедур, обеспечивающих требуемую степень безопасности. Это касается выбора операционных систем, систем управления базами данных (СУБД), прикладного программного обеспечения, среды доставки информации.

Логический уровень характеризует адекватность логических основ механизма безопасности и организации хранения и кодирования информации.

Человеческий уровень отражает степень квалификации и ответственности персонала на стадиях проектирования системы и ее эксплуатации (техническое и программное сопровождение, информационное наполнение, соблюдение требований безопасности).

Законодательный уровень определяет комплекс законодательных и нормативно-правовых актов, регулирующих отношения субъектов в процессах информационного обмена.

Организационный уровень предусматривает комплекс организационных мероприятий, регламентирующий процессы эксплуатации информационной системы.

Структура правовой защиты информации

Реалии современного информационного общества однозначно показывают, что ни одна сфера жизни цивилизованного государства не может эффективно функционировать без развитой информационной инфраструктуры, широкого применения аппаратно-программных средств и современных технологий обработки информации. По мере возрастания ценности информации, развития и усложнения средств ее обработки безопасность общества все в большей степени зависит от безопасности используемых информационных технологий. Многочисленные примеры показывают, что способы злоупотреблений информацией, циркулирующей в различных системах, совершенствуются более интенсивно, чем меры защиты от них. В конце XX века формируются основы теории обеспечения информационной безопасности как направления научных исследований. Теория приобретает определенную структуру, организуются специализированные институты и международные сообщества исследователей, проводятся тематические научные конференции. **В настоящее время для обеспечения защиты информации требуется не просто разработка частных механизмов защиты, а реализация системного подхода, включающего в себя комплекс взаимосвязанных мер с использованием специальных аппаратно-программных средств, организационных мероприятий, нормативно-правовых актов.**

Внутригосударственное право и три основных вопроса, на которые оно отвечает

Что защищать?

- Государственные документы
  - Доктрины, Стратегии
  - Конституция, Законы, Указы, Постановления
- Организационно-распорядительные документы
  - Концепции, Положения, Стандарты

Система защиты информации, правовое пространство, категории информации, права и обязанности обладателя информации, распределение функций, задач, прав и обязанностей между органами госвласти. Система государственных регуляторов.

Как защищать?

- Специальные нормативные документы.
  - Руководства, Приказы, Требования, Методики, Нормы, Критерии защиты, ГОСТ-ы

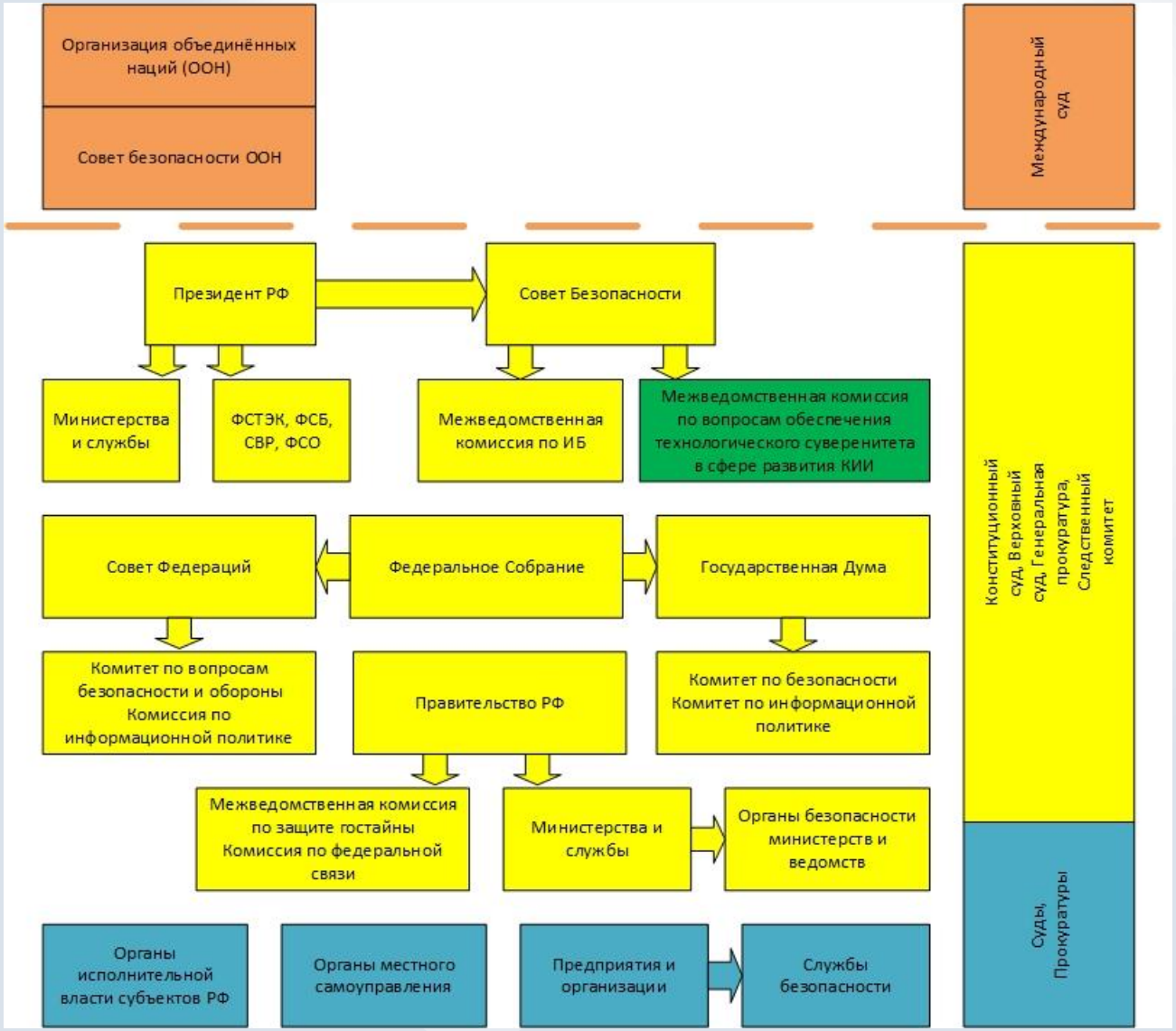
Термины и определения, единство понимания, унификация и стандартизация.

Кому защищать?

- Документы министерства, ведомства, субъекта РФ
  - Руководства, Приказы, Концепции, Положения, Инструкции, Стандарты
- Собственные документы организации
  - Руководства, Приказы, Инструкции, Положения, Стандарты и др.

Отражение отраслевой специфики, региональных особенностей, не противоречащее государственным нормативно-правовым актам.

Организационная структура системы обеспечения ИБ

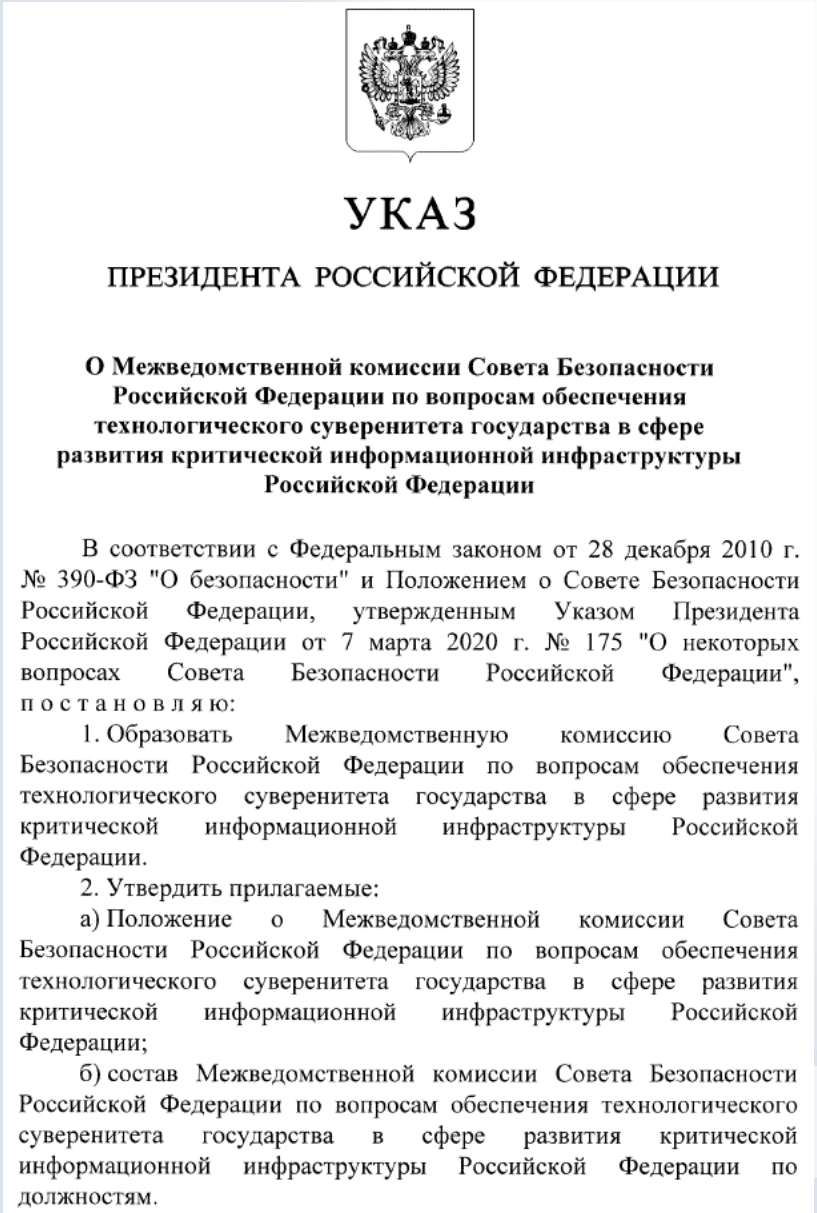


Учитывая глобальный характер процессов информатизации и появление международной киберпреступности, мировое сообщество должно иметь межгосударственные организационные структуры по координации работ в области ИБ.

Основным международным органом является ООН и созданный ею Совет Безопасности. Эти органы координируют усилия государств по осуществлению мероприятий в области обеспечения ИБ и борьбы с преступлениями в сфере ИТ. Спорные вопросы на межгосударственном уровне решает Международный суд.

Система обеспечения ИБ РФ строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти федерального уровня, уровня субъектов РФ, ведомственных структур, а также служб предприятий и организаций. Федеральные министерства и ведомства могут в своем составе создавать соответствующие службы и подразделения для решения вопросов обеспечения информационной безопасности на отраслевом уровне.
Следующим уровнем в системе обеспечения информационной безопасности являются органы исполнительной власти субъектов РФ, органы местного самоуправления, которые могут также создавать различные комиссии.

Актуальные изменения в организационной структуре системы обеспечения ИБ в части КИИ



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации

В соответствии с Федеральным законом от 28 декабря 2010 г. № 390-ФЗ "О безопасности" и Положением о Совете Безопасности Российской Федерации, утвержденным Указом Президента Российской Федерации от 7 марта 2020 г. № 175 "О некоторых вопросах Совета Безопасности Российской Федерации", п о с т а н о в л я ю:

1. Образовать Межведомственную комиссию Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации.

2. Утвердить прилагаемые:

а) Положение о Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации;

б) состав Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации по должностям.

14 апреля 2022 г. Президент РФ подписал указ № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации»

В соответствии с Федеральным законом от 28 декабря 2010 г. № 390-ФЗ "О безопасности" и Положением о Совете Безопасности Российской Федерации, утвержденным Указом Президента Российской Федерации от 7 марта 2020 г. № 175 "О некоторых вопросах Совета Безопасности Российской Федерации", постановляю:

1. Образовать **Межведомственную комиссию Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации**.

2. Утвердить прилагаемые:

а) Положение о Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации;

б) состав Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации по должностям.

3. Председателю Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации в месячный срок утвердить персональный состав Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации.

4. Настоящий Указ вступает в силу со дня его подписания.

НПА. Стратегии.

Стратегия национальной безопасности Российской Федерации

Указом Президента Российской Федерации **от 2 июля 2021 г.** утверждена и вступила в силу обновленная «Стратегия национальной безопасности Российской Федерации». Новый национальный приоритет – информационная безопасность (ИБ) – впервые вошёл в обновлённую стратегию национальной безопасности России.

Стратегия является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты РФ, цели и задачи государственной политики в области обеспечения национальной безопасности и устойчивого развития РФ на долгосрочную перспективу. Предыдущая версия Стратегии национальной безопасности России была опубликована в конце 2015 года. В ней ИБ не выделалась в отдельное направление, она входила в приоритет «наука, технологии и образование». Выделение ИБ в качестве нового приоритета национальной безопасности вызвано более активным, чем прежде, проявлением этих угроз. Соблюдение ИБ должно обеспечить суверенитет страны в информационном пространстве.

Стратегия развития электронной промышленности РФ на период до 2030 г.

Распоряжением Правительства РФ **от 17 января 2020 г. № 20-р** «О Стратегии развития электронной промышленности РФ на период до 2030 г. и плане мероприятий по ее реализации» утверждены:

- Стратегия развития электронной промышленности Российской Федерации на период до 2030 года (далее - Стратегия);

- план мероприятий по реализации Стратегии развития электронной промышленности Российской Федерации на период до 2030 года.

«Стратегия развития электронной промышленности на период до 2030 года (далее - Стратегия)» определяет основные направления государственной политики в сфере развития электронной промышленности Российской Федерации на период до 2030 года.

НПА. Доктрины.

Доктрина информационной безопасности Российской Федерации

Указом Президента РФ **№ 646 от 5 декабря 2016 года** утверждена «Доктрина информационной безопасности Российской Федерации», которая представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере и является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

Доктрина энергетической безопасности Российской Федерации

Указом Президента РФ **№ 216 от 13 мая 2019 года** утверждена обновлённая «Доктрина энергетической безопасности Российской Федерации» - документ стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором отражены официальные взгляды на обеспечение энергетической безопасности Российской Федерации. В Доктрине отмечено:

- **одной из основных трансграничных угроз обозначено** «*противоправное использование информационно-телекоммуникационных технологий, в том числе осуществление компьютерных атак на объекты информационной инфраструктуры и сети связи, используемые для организации их взаимодействия, способное привести к нарушениям функционирования инфраструктуры и объектов топливно-энергетического комплекса*»;

- **одним из основных рисков названо** «*несоответствие технологического уровня российских организаций топливно-энергетического комплекса современным мировым требованиям и чрезмерная зависимость их деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков*»

НПА. Федеральные законы в области защиты информации

Название	Дата принятия
О техническом регулировании	Федеральный закон от 27 декабря 2002 года № 184-ФЗ
Об информации, информационных технологиях и о защите информации	Федеральный закон от 27 июля 2006 года № 149-ФЗ
О государственной тайне	Закон РФ от 21 июля 1993 г. N 5485-I
О лицензировании отдельных видов деятельности	Закон РФ от 04.05.2011 № 99−ФЗ
Кодекс Российской Федерации об административных правонарушениях	От 30 декабря 2001 года № 195-ФЗ
Уголовный кодекс Российской Федерации	От 13 июня 1996 года № 63-ФЗ
Об электронной подписи	Федеральный закон от 6 апреля 2011 года № 63-ФЗ
О федеральной службе безопасности	Закон Российской Федерации № 40 от 3 апреля 1995г.
О персональных данных	Федеральный закон от 27 июля 2006 года № 152-ФЗ
О коммерческой тайне	Федеральный закон от 29 июля 2004 года N 98-ФЗ
О безопасности критической информационной инфраструктуры Российской Федерации	Федеральный закон от 26 июля 2017 года № 187-ФЗ

НПА. Федеральные законы.

Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

01.01.2018 вступил в действие Федеральный закон **№ 187-ФЗ** «О безопасности критической информационной инфраструктуры Российской Федерации». Этим законом определяются основы и принципы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации, в том числе основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на российские информационные ресурсы, которая представляет собой единый территориально распределённый комплекс, включающий в себя силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, механизм предупреждения компьютерных инцидентов на российских объектах КИИ, устанавливаются права и обязанности субъектов КИИ, а также вводится институт категорирования объектов КИИ.

Согласно 187-ФЗ к субъектам КИИ относятся *«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, 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»*.

НПА. 187-ФЗ. Термины и определения.

Автоматизированная система управления - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

Безопасность критической информационной инфраструктуры - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак [8];

Значимый объект критической информационной инфраструктуры - объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

Компьютерный инцидент - факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

Критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

Объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

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, 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.

НПА. Постановления Правительства РФ.

Постановление Правительства РФ № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации»

17.07.2015 г. вышло Постановление Правительства РФ **№ 719** «О подтверждении производства промышленной продукции на территории Российской Федерации», которое определило:

- критерии подтверждения производства промышленной продукции на территории Российской Федерации;

- правила выдачи заключения о подтверждении производства промышленной продукции на территории Российской Федерации;

- порядок формирования и ведения реестра промышленной продукции, произведенной на территории Российской Федерации.

31.12.2020 г. вышло Постановление Правительства РФ № 2458 «О внесении изменений в приложение к постановлению Правительства Российской Федерации от 17 июля 2015 г. № 719», которое, конкретизировало требования к микропроцессорам и микроконтроллерам российского происхождения и, как следствие, к содержащей их продукции, а именно:

- Интегральная схема первого уровня (ИС 1 уровня)
- Интегральная схема второго уровня (ИС 2 уровня)

Пример ИС 1 и 2 уровня. Российские микропроцессоры

Приведём пример отечественных микропроцессоров «Эльбрус» (архитектура VLIW) и «Байкал-М» (архитектура ARM). Согласно ПП РФ № 2458 при наличии технологических возможностей производства указанных микросхем на территории РФ микропроцессоры линейки «Эльбрус» будут относиться к ИС 1 уровня, т.к. имеют собственную архитектуру и систему команд, разработанную в России, а микропроцессоры «Байкал» - к ИС 2 уровня, т.к. имеют лицензию на архитектуру, приобретенную у транснациональной компании ARM (Advanced RISC Machines), со штаб-квартирой, расположенной в Кембридже, Великобритания. **Это различие важно понимать, так как в перспективе возможны законодательные ограничения на применение ИС 2 уровня на объектах КИИ разных категорий.**

НПА. Постановления Правительства РФ.

Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

1. Настоящие Правила устанавливают порядок и сроки категорирования объектов критической информационной инфраструктуры Российской Федерации (далее соответственно - критическая информационная инфраструктура, категорирование).

2. Категорирование осуществляется субъектами критической информационной инфраструктуры в отношении принадлежащих им на праве собственности, аренды или ином законном основании объектов критической информационной инфраструктуры.

3. 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".

НПА. Государственные регуляторы.

ФСТЭК России

Указ Президента РФ от 16 августа 2004 года N 1085 ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по 5 вопросам

Обеспечение защиты (некриптографическими методами) информации

ФСБ России

Федеральный закон от 3 апреля 1995 г. N 40-ФЗ «О федеральной службе безопасности» ФСБ России – единая централизованная система органов федеральной службы безопасности, осуществляющая решение в пределах своих полномочий задач по обеспечению безопасности Российской Федерации

Обеспечение информационной безопасности

Государственный регулятор. ФСТЭК России.

В соответствии с Указом Президента РФ от **16 августа 2004 г. N 1085** «Вопросы Федеральной службы по техническому и экспортному контролю» Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура);

2) противодействия иностранным техническим разведкам на территории Российской Федерации (далее – противодействие техническим разведкам);

3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации (далее - техническая защита информации);

4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

5) осуществления экспортного контроля.

НПА. Приказы ФСТЭК России.

- **Приказ ФСТЭК от 06.12.2017 г. № 227** «Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»
- **Приказ ФСТЭК от 21.12.2017 г. № 235** «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- **Приказ ФСТЭК от 25.12.2017 г. № 239** «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации;
- **Приказ ФСТЭК от 03.04.2018 г. № 55** «Об утверждении Положения о системе сертификации средств защиты информации»;
- **Приказ ФСТЭК от 02.06.2020 г. № 76** «Об утверждении требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий».

НПА. Приказы ФСТЭК России.

- **Приказ ФСТЭК от 14.03.2014 г. № 31** (в ред. Приказов ФСТЭК России от 23.03.2017 № 49, от 09.08.2018 № 138) «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»;
- **Приказ ФСТЭК от 15.03.2021 г. № 46** «О внесении изменений в 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, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31»;
- **Приказ ФСТЭК от 10.02.2022 г. № 26** «О внесении изменений в порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённый Приказом Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 года № 227»

Государственный регулятор. ФСБ России.

В соответствии с Федеральным Законом «О Федеральной службе безопасности» от **22 февраля 1995 г. № 40-ФЗ** направления деятельности органов федеральной службы безопасности применительно к вопросам ИБ определены в:

Статья 11.2. Обеспечение информационной безопасности

Обеспечение информационной безопасности - деятельность органов федеральной службы безопасности, осуществляемая ими в пределах своих полномочий:

- при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;
- при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях, находящихся за пределами Российской Федерации.

Статья 12. Обязанности органов федеральной службы безопасности

и.1) организовывать и обеспечивать безопасность в сфере шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и в пределах своих полномочий в ее учреждениях, находящихся за пределами Российской Федерации;

к) участвовать в разработке и реализации мер по защите сведений, составляющих государственную тайну; осуществлять контроль за обеспечением сохранности сведений, составляющих государственную тайну, в государственных органах, воинских формированиях, на предприятиях, в учреждениях и организациях независимо от форм собственности; в установленном порядке осуществлять меры, связанные с допуском граждан к сведениям, составляющим государственную тайну.

Статья 13. Права органов Федеральной службы безопасности

ш) осуществлять в соответствии со своей компетенцией регулирование в области разработки, производства, реализации, эксплуатации шифровальных (криптографических) средств и защищенных с использованием шифровальных средств систем и комплексов телекоммуникаций, расположенных на территории Российской Федерации, а также в области предоставления услуг по шифрованию информации в Российской Федерации, выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах;

щ) осуществлять государственный контроль за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи, контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории Российской Федерации и в ее учреждениях, находящихся за пределами Российской Федерации, а также в соответствии со своей компетенцией контроль за обеспечением защиты особо важных объектов (помещений) и находящихся в них технических средств от утечки информации по техническим каналам

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

- **Указ Президента Российской Федерации от 15.01.2013 г. № 31с** «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

- **Указ Президента Российской Федерации от 12.12.2014 № К 1274** «О концепции ГосСОПКА»

- **Указ Президента Российской Федерации от 22.12.2017 г. № 620** «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

Основными задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации являются:
а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;
б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;
в) осуществление контроля степени защищенности **критической информационной инфраструктуры** Российской Федерации от компьютерных атак;
г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

НПА. Приказы ФСБ России.

- **Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 366** «О Национальном координационном центре по компьютерным инцидентам»
- **Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 367** «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
- **Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 368** «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

Национальный координационный центр по компьютерным инцидентам(НКЦКИ).

Национальный координационный центр по компьютерным инцидентам (НКЦКИ) является составной частью сил, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и реагирования на компьютерные инциденты. НКЦКИ обеспечивает координацию деятельности субъектов КИИ Российской Федерации по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

К основным функциям НКЦКИ относятся:

- координация мероприятий по реагированию на компьютерные инциденты и непосредственное участие в них;
- участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак;
- доведение до субъектов КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения;
- сбор, хранение и анализ информации о компьютерных инцидентах и компьютерных атаках, а также анализ эффективности мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

НПА. ГОСТ-ы.

- **ГОСТ 34.10-2018** «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
- **ГОСТ 34.11-2018** «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- **ГОСТ 34.12-2018** «Информационная технология. Криптографическая защита информации. Блочные шифры»;
- **ГОСТ 34.13-2018** «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»

- **ГОСТ Р 59853-2021** «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»
- **ГОСТ Р 56939-2016** «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

НПА. Федеральные реестры.

Единый реестр российских программ для электронных вычислительных машин и баз данных

Единый реестр российских программ для электронных вычислительных машин и баз данных создан в соответствии со статьей 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации» в целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки.

Адрес реестра **https://reestr.digital.gov.ru/**

Реестр промышленной продукции, произведенной на территории Российской Федерации

Реестр промышленной продукции, произведенной на территории Российской Федерации создан во исполнение Постановления Правительства Российской Федерации от 17 июля 2015 г. № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации».

Заключение о подтверждении производства промышленной продукции на территории Российской Федерации выдается Минпромторгом России в соответствии с Правилами выдачи заключения о подтверждении производства промышленной продукции на территории Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 17 июля 2015 г. № 719.

Адрес реестра **https://gisp.gov.ru/pp719v2/pub/prod/**

НПА. Федеральные реестры.

Название реестра	Ссылка
Реестры ФСТЭК России	
Государственный реестр сертифицированных средств защиты информации	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00
Реестр лицензий на деятельность по технической защите конфиденциальной информации (ТЗКИ)	https://reestr.fstec.ru/reestr-litsenzij-tzki
Реестр лицензий на деятельность по разработке и производству средств защиты конфиденциальной информации (СЗКИ)	https://reestr.fstec.ru/reestr-litsenzij-szki
Банк данных угроз (БДУ) безопасности информации (угрозы)	https://bdu.fstec.ru/threat
Банк данных угроз (БДУ) безопасности информации (уязвимости)	https://bdu.fstec.ru/vul
Реестры ФСБ России	
Перечень средств защиты информации, сертифицированных ФСБ России (Выписка)	http://clsz.fsb.ru/clsz/certification.htm
База уязвимостей НКЦКИ (ГосСОПКА)	https://safe-surf.ru/specialists/base-vulnerabilities/

НПА. Кодекс РФ об административных правонарушениях.

Федеральный закон от **26.05.2021 г. № 141-ФЗ** «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» ввел административную ответственность (ст.13.121,19.715) для юридических и должностных лиц за нарушения, связанные с критической информационной инфраструктурой (КИИ):

С **6 июня 2021 года** штраф может быть назначен за:

- Непредставление в ФСТЭК сведений о присвоении объекту КИИ категории значимости или о том, что присваивать ее не нужно. Штраф для юрлиц – **от 50 000 до 100 000 руб.**
- Несоблюдение порядка уведомления ФСБ о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий атак в отношении значимых объектов КИИ. Штраф для юрлиц – **от 100 000 до 500 000 руб.**
- Нарушение правил обмена информацией о компьютерных инцидентах (в частности, между субъектами КИИ). Штраф для юрлиц – **от 100 000 до 500 000 руб.**

Максимальный штраф для должностных лиц по таким нарушениям составит **50 000 руб.**

С **1 сентября 2021 года** штраф может быть назначен за:

- Нарушение требований к созданию и обеспечению работы систем безопасности значимых объектов КИИ. Штраф для юрлиц – **от 50 000 до 100 000 руб.**
- Нарушение требований к обеспечению безопасности этих объектов. Штраф для юрлиц – **от 50 000 до 100 000 руб.**

Штраф для должностных лиц по таким нарушениям составит **от 10 000 до 50 000 рублей**.

Срок давности привлечения к ответственности за все эти нарушения составит **1 год**.

НПА. Уголовный кодекс РФ.

Статья 137. Нарушение неприкосновенности частной жизни

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, **без его согласия** либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации - наказываются штрафом в размере **до 200 000 рублей** или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до 360 часов, либо исправительными работами на срок до 1 года, либо принудительными работами на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо арестом на срок до 4 месяцев, **либо лишением свободы на срок до 2 лет с лишением права занимать определенные должности** или заниматься определенной деятельностью на срок до 3 лет.

2. Те же деяния, совершенные лицом **с использованием своего служебного положения**, - наказываются штрафом в размере **от 100 000 до 300 000 рублей** или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового, либо арестом на срок до шести месяцев, **либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности** или заниматься определенной деятельностью на срок до пяти лет.

НПА. Уголовный кодекс РФ.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан - наказывается штрафом в размере **до 80 000 руб.** или в размере заработной платы или иного дохода осужденного за период до 6 месяцев, либо обязательными работами на срок до 360 часов, либо **исправительными работами на срок до 1 года**.

2. То же деяние, совершенное лицом с использованием своего **служебного положения**, - наказывается штрафом в размере **от 100 000 до 300 000 руб.** или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет, либо обязательными работами на срок до 480 часов, либо принудительными работами на срок до 4 лет, либо арестом на срок до 4 месяцев, либо **лишением свободы на срок до 4 лет**.

Статья 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации

Незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для негласного получения информации, - наказываются штрафом в размере до 200 000 руб. или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо ограничением свободы на срок до 4 лет, либо принудительными работами на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового, либо лишением свободы на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.

НПА. Уголовный кодекс РФ.

Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации
Статья 273. Создание, использование и распространение вредоносных компьютерных программ
Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
Статья 274.1. Неправомерное воздействие на **критическую информационную инфраструктуру** Российской Федерации
Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования

НПА. Уголовный кодекс РФ.

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, - наказываются **принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет** или без такового либо лишением свободы на срок от двух до пяти лет со **штрафом в размере от пятисот тысяч до одного миллиона рублей** или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации, - наказывается **принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей** или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо **лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей** или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

НПА. Уголовный кодекс РФ.

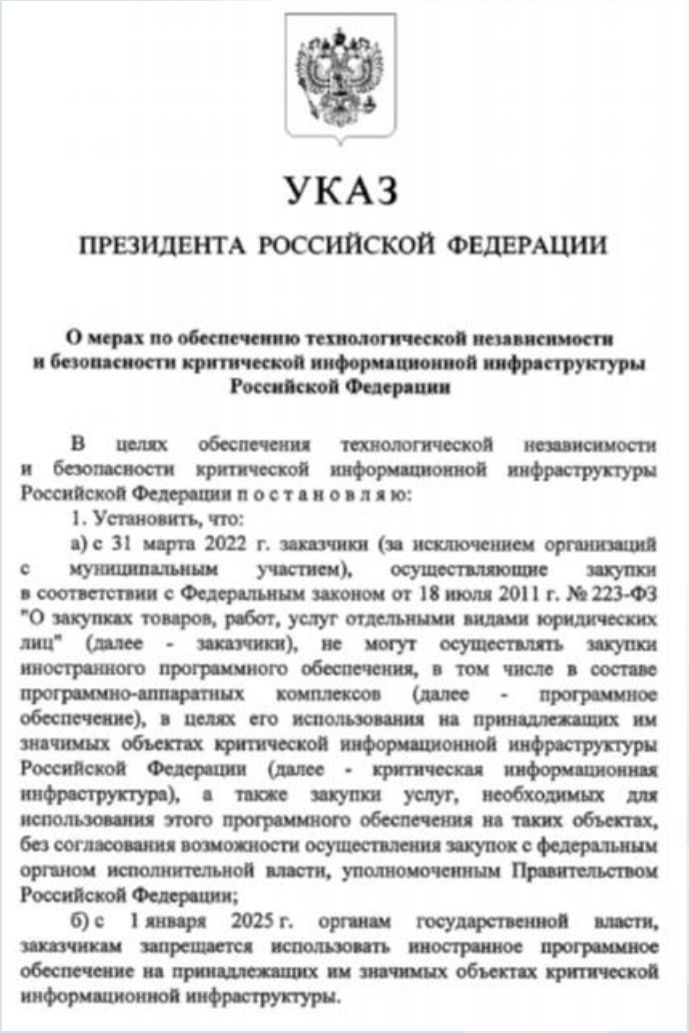
Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, - наказывается **принудительными работами на срок до пяти лет с лишением права занимать определенные должности** или заниматься определенной деятельностью на срок до трех лет или без такового либо **лишением свободы на срок до шести лет с лишением права занимать определенные должности** или заниматься определенной деятельностью на срок до трех лет или без такового.

4. Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, - наказываются **лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности** или заниматься определенной деятельностью на срок до трех лет или без такового.

5. Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия, - наказываются **лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности** или заниматься определенной деятельностью на срок до пяти лет или без такового.

Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации

В целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации п о с т а н о в л я ю:

1. Установить, что:

а) с 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" (далее - заказчики), не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов (далее - программное обеспечение), в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура), а также закупки услуг, необходимых для использования этого программного обеспечения на таких объектах, без согласования возможности осуществления закупок с федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации;

б) с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.

1а. **С 31 марта 2022 г.** заказчики (за исключением организаций с муниципальным участием), не могут осуществлять закупки (по 223-ФЗ) без согласования с федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации:

- иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования на принадлежащих им значимых объектах **критической информационной инфраструктуры (ЗОКИИ)**
- услуг, необходимых для использования этого программного обеспечения на принадлежащих им **ЗОКИИ**

1б. **С 1 января 2025 г.** органам государственной власти, заказчикам запрещается использование иностранного программного обеспечения на принадлежащих им **ЗОКИИ**

2б. В **6-месячный срок** реализовать комплекс мероприятий, направленных на обеспечение **преимущественного применения субъектами КИИ отечественных радиоэлектронной продукции и телекоммуникационного оборудования на принадлежащих им ЗОКИИ**, в том числе:

- определить сроки и порядок перехода субъектов КИИ на **преимущественное применение доверенных программно-аппаратных комплексов** на принадлежащих им ЗОКИИ;
- обеспечить создание и организацию деятельности научно-производственного объединения, специализирующегося на разработке, производстве, технической поддержке и сервисном обслуживании доверенных программно-аппаратных комплексов для КИИ;

Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О дополнительных мерах по обеспечению информационной безопасности Российской Федерации

В целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации п о с т а н о в л я ю:

1. Руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (далее - органы (организации):

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

б) создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;

1. Руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций, стратегических предприятий … :

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты

б) создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности

2. Возложить на руководителей органов (организаций) персональную ответственность за обеспечение информационной безопасности соответствующих органов (организаций)

6. Установить, что **с 1 января 2025 г.** органам (организациям) **запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства,** совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

Распоряжение Правительства Российской Федерации от 22.06.2022 № 1661-р

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 22 июня 2022 г. № 1661-р

МОСКВА

В соответствии с подпунктом "б" пункта 3 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" утвердить прилагаемый перечень ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России.

Председатель Правительства Российской Федерации

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
4DCB95D0582AAD8E3067B22BF1D3CE444B...
Поставщик: Федеральное казначейство
Правительство Российской Федерации
Действителен с 10.12.2021 по 10.03.2023

М.Мишустин

В соответствии с подпунктом "б" пункта 3 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" утвердить прилагаемый перечень ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России.

Перечень содержит 72 позиции, которые во многом повторяют Указ Президента Российской Федерации № 1009 от 04.08.2004 г. «Об утверждении перечня стратегических предприятий и стратегических акционерных обществ».

Юридически значимое определение термина ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС.

Постановление Правительства РФ № 2461 от 28 декабря 2022 г. «О внесении изменений в Постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 и признании утратившими силу отдельных положений некоторых актов Правительства Российской Федерации» ввело в законодательство РФ юридически значимое определение термина ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС (ПАК):

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС (ПАК) — это комплекс технических и программных средств (программного обеспечения), работающих совместно для выполнения одной или нескольких специальных задач, являющийся электронной вычислительной машиной или специализированным электронным устройством (устройствами), функционально-технические характеристики которого (которых) определяются исключительно совокупностью программного обеспечения и технических средств, и не могут быть реализованы при их разделении. Программно-аппаратный комплекс является самостоятельно используемым, законченным техническим изделием, имеющим серийный номер.

Таким образом с вводом данного юридически значимого определения термин программно-аппаратный комплекс (ПАК), введенный Указом Президента № 166 получил однозначное толкование, а его «ДОВЕРЕННОСТЬ» определяется Приказом ФСТЭК № 76 от 02.06.2020 г.

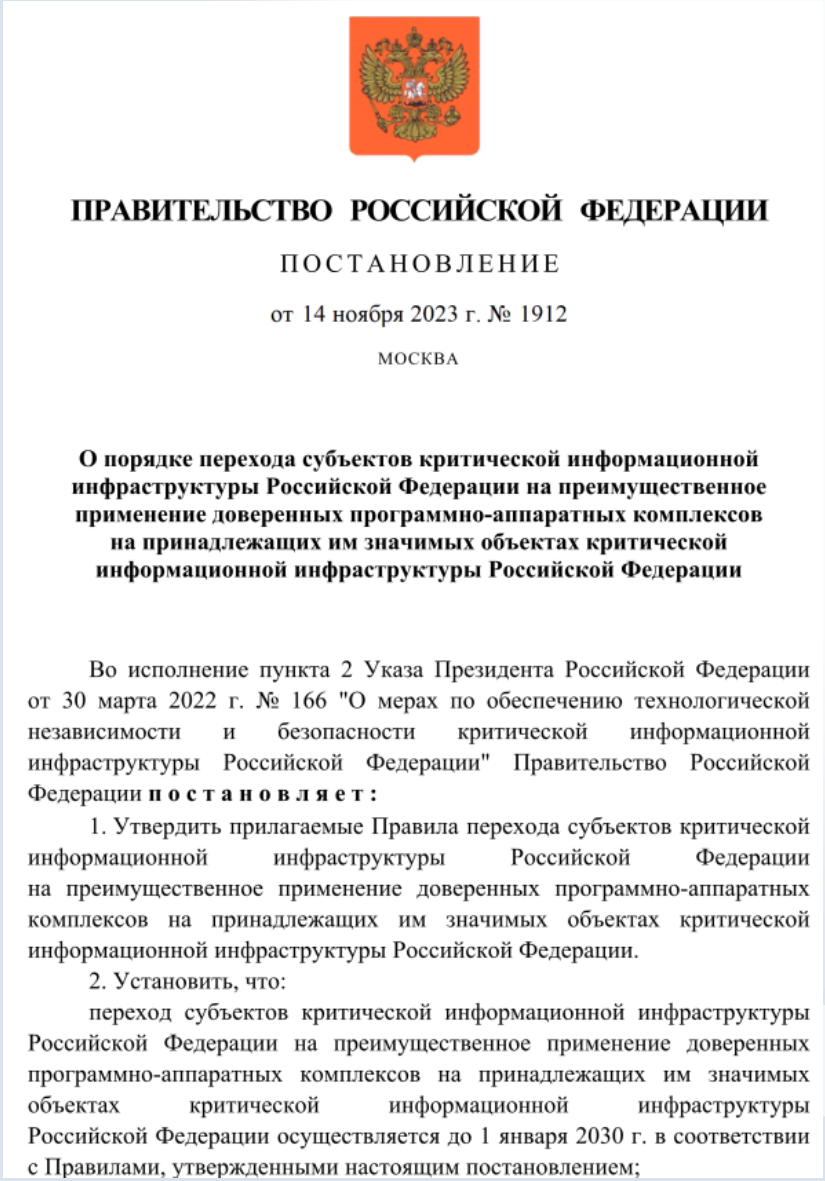
ПНСТ 905-2023 «Критическая информационная инфраструктура. Доверенные программно-аппаратные комплексы. Термины и определения».

28 декабря 2023 года Приказом № 115-пнст Федерального агентства по техническому регулированию и метрологии «Об утверждении предварительного национального стандарта Российской Федерации» утверждён предварительный национальный стандарт Российской Федерации ПНСТ 905-2023 «Критическая информационная инфраструктура. Доверенные программно-аппаратные комплексы. Термины и определения» с датой введения в действие 1 апреля 2024 года и сроком до 1 апреля 2027 года.

ПНСТ-905-2023 закреплён за техническим комитетом по стандартизации № 167 «Программно-аппаратные комплексы для критической информационной инфраструктуры и программное обеспечение для них» (ТК 167).

Таким образом, при выполнении различных работ, выполнении НИОКР применительно к системам технологического управления в составе объектов КИИ, проектировании технических решений, составлении технических заданий и т.д. целесообразно использовать ПНСТ-905-2023 для однозначного толкования предметной области доверенных ПАК для КИИ.

Постановление Правительства Российской Федерации от 14.11.2023 г. № 1912 – важный нормативный акт для ЗОКИИ



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;

Постановление Правительства Российской Федерации от 14.11.2023 г. № 1912 **«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»** определяет ряд важных моментов для ЗОКИИ:

- ✓ Утверждает «**правила перехода субъектов КИИ РФ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им ЗОКИИ**»
- ✓ Определяет, что переход субъектов КИИ РФ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации осуществляется **до 1 января 2030 г.**
- ✓ Не допускается **с 1 сентября 2024 г.** использование субъектами КИИ РФ на принадлежащих им ЗОКИИ программно-аппаратных комплексов, приобретенных субъектами КИИ РФ с 1 сентября 2024 г. и не являющихся доверенными программно-аппаратными комплексами, за исключением случаев отсутствия произведенных в Российской Федерации доверенных программно-аппаратных комплексов, являющихся аналогами приобретенных субъектами КИИ РФ программно-аппаратных комплексов
- ✓ Утверждает, что доля доверенных ПАК на ЗОКИИ по состоянию **на 31 декабря 2029 г.** должна составлять **100 процентов** в общем количестве программно-аппаратных комплексов на ЗОКИИ
- ✓ Вводит критерии доверенного программно-аппаратного комплекса для ЗОКИИ

Постановление Правительства Российской Федерации от 14.11.2023 г. № 1912 – критерии доверенного ПАК для ЗОКИИ

В Приложении 1 к Постановлению Правительства Российской Федерации от 14.11.2023 г. № 1912 **«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»** определяются обязательные критерии к доверенному ПАК.

Их три и доверенный ПАК должен соответствовать одновременно всем критериям:

- ✓ Сведения о доверенном ПАК содержатся в реестре российской радиоэлектронной продукции;
- ✓ Программное обеспечение, используемое в составе доверенного ПАК, соответствует требованиям из Постановления Правительства РФ от 22.08.2022 г. № 1478;
- ✓ ПАК, в случае реализации в нём функции защиты информации соответствует требованиям, установленным ФСТЭК и(или) ФСБ РФ в пределах их полномочий, что должно быть подтверждено соответствующим документом (сертификатом).

Приказ ФСТЭК № 31 (Защита АСУ ТП).

Приказ ФСТЭК от 14.03.2014 г. № 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 приказе **устанавливаются требования** к обеспечению защиты информации, обработка которой осуществляется АСУ ТП на КВО, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (КА), следствием которых может стать нарушение функционирования АСУ ТП. **Требования применяются** в случае принятия владельцем АСУ ТП решения об обеспечении защиты информации, обработка которой осуществляется этой системой и нарушение безопасности которой может привести к нарушению функционирования АСУ ТП. **Действие требований распространяется** на АСУ ТП, обеспечивающие контроль и управление технологическим и (или) производственным оборудованием (исполнительными устройствами) и реализованными на нем технологическими и (или) производственными процессами (в том числе системы диспетчерского управления, системы сбора (передачи) данных, системы, построенные на основе ПЛК, распределенные системы управления, системы управления станками с ЧПУ). **Требования предназначены** для лиц, устанавливающих требования к защите информации в АСУ ТП (ЗАКАЗЧИК), лиц, обеспечивающих эксплуатацию АСУ ТП (ОПЕРАТОР), а также лиц, привлекаемых в соответствии с законодательством Российской Федерации к проведению работ по созданию (проектированию) АСУ ТП и (или) их систем защиты (РАЗРАБОТЧИК).

Обеспечение безопасности АСУ ТП, являющимися ЗОКИИ – Приказ ФСТЭК № 235 и Приказ № 239

Приказ ФСТЭК № 235 (Создание СБ ЗОКИИ).

Приказ ФСТЭК от 21.12.2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

Системы безопасности создаются субъектами КИИ и включают в себя правовые, организационные, технические и иные меры, направленные на обеспечение ИБ субъектов КИИ. Создание и функционирование систем безопасности должно быть направлено на обеспечение устойчивого функционирования ЗОКИИ при проведении в отношении них компьютерных атак. Системы безопасности создаются **в отношении всех ЗОКИИ** субъектов КИИ. **Системы безопасности включают силы** обеспечения безопасности ЗОКИИ **и используемые ими средства** обеспечения безопасности ЗОКИИ. **К силам** обеспечения безопасности ЗОКИИ **относятся**: подразделения (работники) субъекта КИИ, ответственные за обеспечение безопасности ЗОКИИ; подразделения (работники), эксплуатирующие ЗОКИИ; подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) ЗОКИИ иные подразделения (работники), участвующие в обеспечении безопасности ЗОКИИ. **К средствам** обеспечения безопасности ЗОКИИ **относятся** программные и программно-аппаратные средства, применяемые для обеспечения безопасности ЗОКИИ. **Системы безопасности должны обеспечивать**: **предотвращение неправомерного доступа** к информации, обрабатываемой ЗОКИИ, **уничтожения** такой информации, ее **модифицирования, блокирования, копирования, предоставления и распространения**, а также иных неправомерных действий в отношении такой информации; **недопущение воздействия** на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование ЗОКИИ; **восстановление функционирования** ЗОКИИ, в том числе за счет создания и хранения резервных копий необходимой для этого информации; непрерывное взаимодействие с ГосСОПКА, которое осуществляется в соответствии со статьей 5 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

Приказ ФСТЭК № 239 (Жизненный цикл ОКИИ).

Приказ ФСТЭК от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Действие Требований распространяется на информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, которые отнесены к ЗОКИИ в соответствии со ст.7 № 187-ФЗ от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации». По решению субъекта КИИ **Требования могут применяться** для обеспечения безопасности ОКИИ, не отнесенных к ЗОКИИ. Обеспечение безопасности ЗОКИИ является составной частью работ по созданию (модернизации), при которой изменяется архитектура ЗОКИИ, в том числе подсистема его безопасности, в соответствии с отдельным техническим заданием на модернизацию ЗОКИИ и (или) техническим заданием (частным техническим заданием) на модернизацию подсистемы безопасности ЗОКИИ, эксплуатации и вывода из эксплуатации ЗОКИИ. **Меры по обеспечению безопасности ЗОКИИ принимаются на всех стадиях (этапах) их жизненного цикла.** Для ЗОКИИ, находящихся в эксплуатации, **Требования подлежат реализации** в рамках модернизации или дооснащения подсистем безопасности эксплуатируемых ЗОКИИ. Модернизация или дооснащение подсистем безопасности ЗОКИИ осуществляется в порядке, установленном Требованиями для создания ЗОКИИ и их подсистем безопасности, с учетом имеющихся у субъектов КИИ программ (планов) по модернизации или дооснащению ЗОКИИ. Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ осуществляется субъектом КИИ и (или) лицом, привлекаемым в соответствии с законодательством Российской Федерации к проведению работ по созданию (модернизации) ЗОКИИ и (или) обеспечению его безопасности, в соответствии с техническим заданием на создание ЗОКИИ и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности ЗОКИИ и должна включать:

а) **анализ угроз безопасности** информации и **разработку модели угроз безопасности** информации или ее уточнение (при ее наличии);

б) проектирование подсистемы безопасности ЗОКИИ;

в) разработку рабочей (эксплуатационной) документации на ЗОКИИ (в части обеспечения его безопасности).

Приказ ФСТЭК № 26 (Рег. № ЗОКИИ).

Приказ ФСТЭК от 10.02.2022 г. № 26 «О внесении изменений в порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённый Приказом Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 года № 227»

Каждому ЗОКИИ, включенному в Реестр, присваивается регистрационный номер, состоящий из групп цифр и прописных букв, разделенных косыми чертами, который имеет вид: **XXXXXX/X/XX/X**.

Первая группа знаков содержит число от 000001 до 999999, указывающее на порядковый номер значимого объекта критической информационной инфраструктуры в Реестре.

Вторая группа знаков содержит число, обозначающее федеральный округ, на территории которого ЗОКИИ:

1 - Центральный федеральный округ;
2 - Северо-Западный федеральный округ;
3 - Южный федеральный округ;
4 - Северо-Кавказский федеральный округ;
5 - Приволжский федеральный округ;
6 - Уральский федеральный округ;
7 - Сибирский федеральный округ;
8 - Дальневосточный федеральный округ.

Третья группа знаков содержит двузначное число, обозначающее сферу (область) деятельности, в которой функционирует значимый объект критической информационной инфраструктуры, определенную в соответствии с пунктом 8 статьи 2 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации":

1 - здравоохранение; 2 - наука; 3 - транспорт; 4 - связь; 5 - банковская сфера и иные сферы финансового рынка; **6 - энергетика**; **7 - атомная энергия**; 8 - оборонная промышленность; 9 - ракетно-космическая промышленность; 10 - горнодобывающая промышленность; 11 - металлургическая промышленность; 12 - химическая промышленность; **13 - топливно-энергетический комплекс (за исключением энергетики).**

Четвертая группа знаков содержит прописную букву, которая обозначает тип значимого объекта критической информационной инфраструктуры: "А" - информационная система; "Б" - автоматизированная система управления технологическими (производственными) процессами; "В" - информационно-телекоммуникационная сеть.

Методика оценки угроз безопасности информации (ФСТЭК России).

Методика оценки угроз безопасности информации разработана в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, и утверждена ФСТЭК России **5 февраля 2021 года**.

Методика определяет порядок и содержание работ по определению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах, а также по разработке моделей угроз безопасности информации систем и сетей.

Методика применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, **значимым объектам критической информационной инфраструктуры Российской Федерации**, информационным системам управления производством, используемым организациями оборонно-промышленного комплекса, автоматизированным системам управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

На основе **Методики** могут разрабатываться отраслевые (ведомственные, корпоративные) методики оценки угроз безопасности информации, которые учитывают особенности функционирования систем и сетей в соответствующей области деятельности. **Разрабатываемые отраслевые (ведомственные, корпоративные) методики оценки угроз безопасности информации не должны противоречить положениям Методики**.

Методика оценки угроз безопасности информации (ФСТЭК России).

Оценка угроз безопасности информации проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях с заданной архитектурой и в условиях их функционирования – актуальных угроз безопасности информации.

Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

а) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

б) инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;

в) определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

г) оценка способов реализации (возникновения) угроз безопасности информации;

д) оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

е) оценка сценариев реализации угроз безопасности информации в системах и сетях.

Методика оценки угроз безопасности информации ФСТЭК России – руководство к действию по составлению двух важных документов в вашей организации: МОДЕЛИ УГРОЗ и МОДЕЛИ НАРУШИТЕЛЯ.

Законодательные инициативы, направленные на импортозамещение

В перечне Министерства промышленности и торговли РФ «Перечень приоритетных и критических видов продукции, услуг и программного обеспечения, с точки зрения импортозамещения и национальной безопасности», по элементам релейной защиты и АСУ ТП дана характеристика **«Критично. Высокая зависимость от импортных комплектующих»**.

Следует отметить, что российские производители устройств релейной защиты и АСУ ТП в настоящее время используют исключительно импортные критичные с точки зрения ИБ компоненты.

Импортозамещение. Детализация Приказа ФСТЭК от 02.06.2020 г. № 76.

В соответствии с Постановлением Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» большинство объектов ПАО «Россети» должно быть отнесено к ЗОКИИ.

Уровень доверия	Категория ЗОКИИ	Обязательно для:
6-й уровень	3 категория	АСУ ТП 3 класса защищённости
5-й уровень	2 категория	АСУ ТП 2 класса защищённости
4-й уровень	**1 категория**	**АСУ ТП 1 класса защищённости**

Требования к средствам 4,5,6-го уровней доверия, в данном случае к РЗА и АСУ ТП, практически не отличаются, таким образом они должны быть сертифицированы по 4-му уровню доверия для эксплуатации на объектах ЗОКИИ 1 категории.

Импортозамещение. Детализация Приказа ФСТЭК от 02.06.2020 г. № 76 .

Согласно **«Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (Приказ ФСТЭК России от 2 июня 2020 г. № 76)** вторичное оборудование, которое эксплуатируется в контуре АСТУ на ОКИИ в ПАО «Россети», должно быть сертифицировано ФСТЭК по 4УД.

Вышеуказанные «Требования…» определяют:

- с **1 января 2022 г.** (п.п. 12.2, 12.4) обязательным становится применение отечественных аппаратных платформ СЗИ (с 5 уровня доверия) и СВТ, являющихся средой функционирования СЗИ (с 3 уровня доверия);
- с **1 января 2024 г.** (п. 12.3) обязательным становится применение отечественных процессоров, микросхем, элементов памяти, сетевых карт, графических адаптеров СЗИ (с 4 уровня доверия);
- с **1 января 2028 г.** (п. 12.5) обязательным становится применение отечественных процессоров, микросхем, элементов памяти, сетевых карт, графических адаптеров СВТ, являющихся средой функционирования СЗИ (с 2 уровня доверия).

НПА. Отраслевые документы по ИБ объектов электроэнергетики (ОКИИ).

Название	Дата принятия
Положение ПАО «Россети» о единой технической политике в электросетевом комплексе	Решение Совета директоров ПАО «Россети», протокол заседания от 02.04.2021 № 450
Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса группы компаний «Россети»	Распоряжение ПАО «Россети» № 282р от 30.05.2017 г.
Об утверждении требований по обеспечению безопасности информации микропроцессорных устройств релейной защиты и автоматики	Распоряжение ПАО «Россети» № 62р от 28.02.2022 г.
Методика проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе	Приказ ПАО «Россети» № 391 от 28.08.2020 г.
СТО 34.01-21-004-2019 ПАО «Россети» «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110–220 кВ и узловых цифровых подстанций напряжением 35 кВ»	Приказ ПАО «Россети» № 64 29.03.2019 г.
СТО 34.01-21-005-2019 ПАО «Россети» «Цифровая электрическая сеть. Требования к проектированию цифровых распределительных электрических сетей 0,4-220 кВ»	Приказ ПАО «Россети» № 64 29.03.2019 г.
СТО 56947007-29.240.10.256-2018 «Технические требования к аппаратно-программным средствам и электротехническому оборудованию ЦПС»	Приказ ПАО «Россети» № 355 от 21.09.2018 г.
Документ «ПЕРЕЧЕНЬ ТИПОВЫХ ОТРАСЛЕВЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ, ФУНКЦИОНИРУЮЩИХ В СФЕРЕ ЭНЕРГЕТИКИ» (https://minenergo.gov.ru/opendata/7715847529-perechen-obektov-kii-2023)	Рекомендации Министерства энергетики РФ, Первичная публикация 08.08.2023 г.

Выводы

1. При разработке технических заданий на выполнения НИР и НИОКР в обязательном порядке учитывать требования государственных и отраслевых нормативных документов по информационной безопасности.

2. Разработку технических решений НИР и НИОКР, касающихся объектов критической информационной инфраструктуры, необходимо реализовать с исполнением специальных разделов, отражающих организационные и технические мероприятия по обеспечению их информационной безопасности.

3. Допускать к участию в конкурсах на разработку цифровых устройств и программного обеспечения для объектов критической информационной инфраструктуры электросетевого комплекса только специализированные организации, имеющие лицензии ФСТЭК.

4. При выполнении НИОКР для значимых объектов критической информационной инфраструктуры с разработкой цифровых устройств и программного обеспечения осуществлять приемку только **доверенных** ПАК, отвечающих требованиям Постановления Правительства №1912 от 14.11. 2023 года.

СПАСИБО ЗА ВНИМАНИЕ !

Контакты:

Куликов Александр Леонидович

E-MAIL: inventor61@mail.ru