Вопросы совершенствования нормативного правового регулирования системы защиты информационных ресурсов Союзного государства



Программы Союзного Государства

- Защита общих информационных ресурсов Беларуси и России
- 2000 2005 годы
- Совершенствование системы защиты общих информационных ресурсов Беларуси и России
- 2006 2010 годы
- Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий
- 2011 2015 годы



Программы Союзного Государства

 Совершенствование системы защиты информационных ресурсов Союзного государства и государств-участников Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере

выявление и описание угроз безопасности информации, связанных с использованием новых ИТ

создание защищенных трансграничных ИС Союзного государства

изыскание новых технических решений по созданию СЗИ

разработка рекомендаций по ЗИ и способов ее защиты в ИС, построенных с использованием новых ИТ

развитие методического обеспечения мониторинга и прогнозирования угроз безопасности информации в ИС

развитие методического обеспечения организации защиты и построения СЗИ в ИС путем создания SIEMсистемы

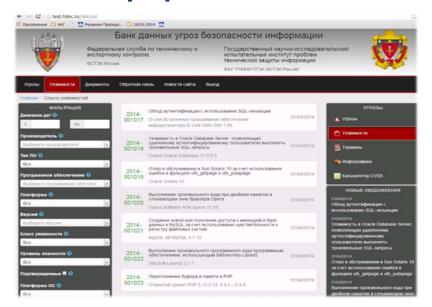
совершенствование технического регулирования в области защиты ИС от современных угроз безопасности информации

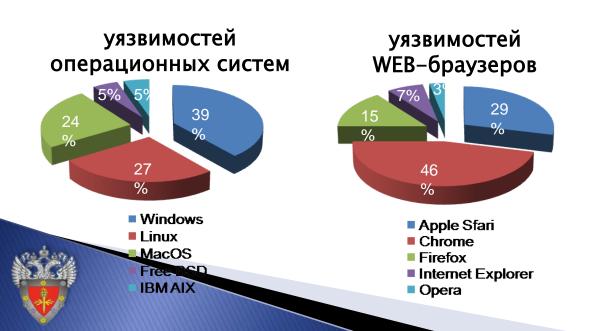


Банк данных угроз безопасности информации

более 18500 уязвимостей информационных технологий

208 угрозы безопасности информации





уязвимостей оборудования оборудования отказ в обслуживании выполнение кода переполнение буфера межсайтовое выполнение сценариев Разглашение информации Обход ограничений

Остапьное

ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»



Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» вступил в силу с 1 января 2018 г.



Сфера здравоохранения



Банковская сфера и иные сферы финансового рынка



Сфера горнодобывающей промышленности





Сфера энергетики и топливноэнергетического комплекса



Сфера металлургической промышленности





Сфера транспорта



Сфера атомной энергии



Сфера химической промышленности

Сфера связи



Сфера ракетнокосмической промышленности



Сфера оборонной промышленности





Система нормативных правовых актов в области обеспечения безопасности объектов **критической информационной инфраструктуры Российской Федерации** Федеральный закон от 26 июля 2017 г. № 187-ФЗ

«О безопасности критической информационной инфраструктуры Российской Федерации»

Нормативные правовые акты Президента Российской Федерации

Указ Президента РФ от 25 ноября 2017 г. № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085»

Указ Президента РФ «О внесении изменений в Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации компьютерных атак»

Указ Президента РФ от 2 марта 2018 г. «О внесении изменений в Перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента РФ от 30 ноября 1995 г. № 1203»

Нормативные правовые акты Правительства Российской Федерации

Постановление Правительства РФ «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» от 8 февраля 2018 г. № 127

Постановление Правительства РФ «Об утверждении порядка осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры» от 17 февраля 2018 г. №162

Проект постановления Правительства РФ «Об утверждении порядка подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов КИИ»

Нормативные правовые акты федеральных органов исполнительной власти

Приказ ФСТЭК России «Об утверждении требований к созланию систем безопасности значимых объектов КИИ» от 21 декабря 2017 г. № 235 (зарегистрирован Минюстом России 22 февраля 2018 г., рег. № 50118)

Приказ ФСТЭК России «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости» от 22 декабря 2017 г. № 236 (находится на регистрации в Минюсте России)

Приказ ФСТЭК России «Об утверждении требований по обеспечению безопасности значимых объектов КИИ» от 25 декабря 2017 г. № 239 (зарегистрирован Минюстом России 26 марта 2018 г., рег. № 50524)

Приказ ФСТЭК России «Об утверждении формы акта проверки» от 11 декабря 2017 г. № 229 (зарегистрирован Минюстом России 28 декабря 2017 г., рег. № 49500)

Приказ ФСТЭК России «Об утверждении порядка ведения реестра значимых объектов КИИ» от 6 декабря 2017 г. № 227 (зарегистрирован Минюстом России 8 февраля 2018 г., рег. № 49966)

Приказ ФСБ России «Об утверждении Положения о Национальном координационном центре по компьютерным инцидентам»

Приказ ФСБ России «Об утверждении перечня информации, представляемой в ГосСОПКА и порядка ее представления»

Приказ ФСБ России «Об утверждении порядка информирования ФСБ России о компьютерных инцидентах и реагирования на них»

Приказ ФСБ России «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак»

Приказ ФСБ России «Об утверждении порядка об обмене информации о компьютерных инцидентах между субъектами КИИ»

Приказ Минкомсвязи России «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак на сетях связи»

Приказ ФСБ России «Об утверждении требований к средствам обнаружения, предупреждения и ликвидации компьютерных атак»

Кто является субъектом КИИ?









Общероссийский классификатор видов экономической деятельности

Лицензии и иные разрешительные документы на различные виды деятельности

Уставы, положения организаций (государственных органов)

.





Указ Президента Российской Федерации от 25 ноября 2017 г. № 569

«О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085»

ФСТЭК России является ФОИВ, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам обеспечения безопасности критической информационной инфраструктуры Российской Федерации





Постановление Правительства Российской Федерации 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»

Подготовлено в соответствии с пунктом 1 части 2 статьи 6 Федерального закона № 187-Ф3

Утверждает:

Правила категорирования объектов КИИ РФ

Перечень показателей критериев значимости объектов КИИ РФ и их значения

К обсуждению привлечены представители более 40 организаций

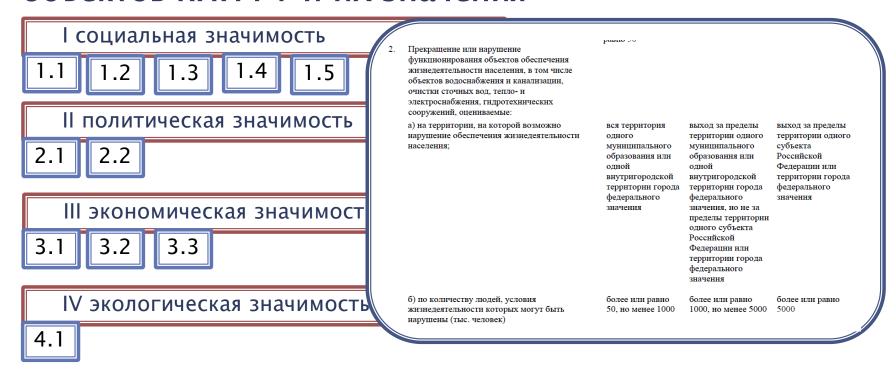
Согласовано с 12 ФОИВ, ЦБ РФ, ГК «Росатом», ГК «Роскосмос»



Правила категорирования объектов КИИ РФ



Перечень показателей критериев значимости объектов КИИ РФ и их значения



V значимость для обеспечения обороны страны, безопасности государства и правопорядка

5.1

5.2

5.3

Оценка производится по <u>каждому</u> из значений!

Категория присваивается по наивысшему значению



Перечень показателей критериев значимости объектов КИИ РФ и их значения

І категория

II категория

III категория

Объекты, для которых отсутствует необходимость присвоения категории значимости

Категории значимости объектов КИИ



Внесение сведений в Реестр значимых объектов КИИ



Направление сведений о результатах категорирования в ФСТЭК России

Пункт 1*7* Правил категорирования



ФСТЭК России

ПРИКАЗ от 22 декабря 2017 г. № 236

Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

сведения об объекте КИИ

сведения о субъекте КИИ

сведения о взаимодействии объекта КИИ и сетей электросвязи

сведения о лице, эксплуатирующем объект КИИ

сведения о программных и программно-аппаратных средствах, используемых на КИИ

сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ

возможные последствия в случае возникновения компьютерных инцидентов на объекте КИИ

категория значимости, которая присвоена объекту КИИ, а также сведения о результатах оценки показателей критериев значимости

организационные и технические меры, применяемые для обеспечения безопасности объекта КИИ



Реестр значимых объектов критической информационной инфраструктуры Российской Федерации



ФСТЭК России

ПРИКАЗ от 6 декабря 2017 г. № 227

Об утверждении
Порядка ведения реестра
значимых объектов
критической информационной
инфраструктуры
Российской Федерации

Формируется и ведется ФСТЭК России

Формируется и ведется на основании сведений, представляемых субъектами КИИ

Подлежит защите в соответствии с законодательством Российской Федерации о государственной тайне

В случае изменения сведений о значимых объектах КИИ, субъекты КИИ направляют измененные сведения в ФСТЭК России



Создание системы безопасности объектов КИИ и внедрение мер по обеспечению защиты объектов КИИ



Приказ ФСТЭК России от 21 декабря 2017 г. № 235

«Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

Подготовлен в соответствии с пунктом 4 части 3 статьи 6 Федерального закона № 187-ФЗ

Устанавливает требования к силам обеспечения безопасности значимых объектов

Устанавливает требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов

Устанавливает требования к организационно-распорядительным документам по безопасности значимых объектов



Создание системы безопасности объектов КИИ и внедрение мер по обеспечению защиты объектов КИИ



Приказ ФСТЭК России от 25 декабря 2017 г. № 239

«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Подготовлен в соответствии с пунктом 4 части 3 статьи 6 Федерального закона № 187-ФЗ

Общие положения

Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов

Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

Приложение. Состав мер по обеспечению безопасности для значимых объектов соответствующей категории



Формы оценки соответствия СЗИ и подтверждения соответствия значимого объекта

Оценка соответствия средств защиты информации





Применяется в случаях, установленных законодательством РФ и по решению субъекта КИИ

Испытания



Приемка



В <u>иных случаях</u> и проводятся <u>самостоятельно</u> или с <u>привлечением</u> <u>организаций-лицензиатов</u>

Подтверждение соответствия значимого объекта

Аттестация



В случаях, если значимый объект – <u>ГИС</u> в соответствии с законодательством <u>РФ</u> и по решению субъекта КИИ Приемочные испытания



В иных случаях



Особенности реализации требований

Значимый > объект КИИ обрабатывает ГТ Законодательство РФ о государственной тайне

Значимый объект КИИ является ГИС

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Приказ ФСТЭК России от 25 декабря 2017 г. № 239

Значимый объект КИИ является ИСПДн Постановление Правительства РФ от 1 ноября 2012 г. № 1119

Приказ ФСТЭК России от 25 декабря 2017 г. № 239

Значимый объект КИИ является ИТКС

Приказ ФСТЭК России от 25 декабря 2017 г. № 239 Нормативные правовые акты Минкомсвязи России

 Приказ ФСТЭК России от 25 декабря 2017 г. № 239



Методические документы ФСТЭК России

Проект



Меры защиты информационных и автоматизированных систем и содержащейся в них информации

Общие положения

Выбор мер защиты информации

Содержание мер защиты информации



Государственный контроль



Постановление Правительства Российской Федерации от 17 февраля 2018 г. №162

«Об утверждении порядка осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры»

Подготовлено в соответствии с пунктом 2 части 2 статьи 6 Федерального закона № 187-ФЗ

Устанавливает правила осуществления ФСТЭК России и ее территориальными органами мероприятий по государственному контролю в области обеспечения безопасности значимых объектов КИИ РФ

Виды контроля: Плановый Внеплановый



Государственный контроль



Приказ ФСТЭК России от 11 декабря 2017 г. № 229

«Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры»

Подготовлен в соответствии с пунктом 5 части 3 статьи 6 Федерального закона № 187-ФЗ

Определяет типовую форму акта проверки







СПАСИБО ЗА ВНИМАНИЕ!



ТОРБЕНКО Елена Борисовна Заместитель начальника управления ФСТЭК России