Направления совершенствования технической защиты информации и обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Заместитель директора ФСТЭК России
Лютиков Виталий Сергеевич

СИСТЕМА НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ 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 от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ»

Указ Президента РФ от 2 марта 2018 г. № 98 «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 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»

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

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

Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости» (зарегистрирован Минюстом России 13 апреля 2018 г., рег. № 50753)

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

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

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

Приказ ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован Минюстом России 6 сентября 2018 г., рег. № 52109)

Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА» (зарегистрирован Минюстом России 6 сентября 2018 г., рег. № 52108)

Проект приказа ФСБ России «Об утверждении порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер ликвидации последствий»

Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ, между субъектами КИИ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (зарегистрирован Минюстом России 6 сентября 2018 г., рег. № 52107)

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

Проект приказа ФСБ России «Об утверждении требований к средствам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»

Проект приказа ФСБ России «Об утверждении порядка, технических условий установки и эксплуатации средств ГосСОПКА»

СОВЕРШЕНСТВОВАНИЕ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КИИ

Федеральный закон

«О внесении изменений в КоАП (в части установления ответственности за нарушение требований по обеспечению безопасности объектов КИИ)»

Постановление Правительства Российской Федерации

«О внесении изменений в Правила категорирования объектов КИИ и перечень показателей критериев значимости КИИ и их значений, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127»

Приказ ФСТЭК России «О внесении изменений в форму направления сведений о результатах категорирования объекта КИИ, утвержденную приказом ФСТЭК России от 22 декабря 2017 г. № 236»

Приказ ФСТЭК России «О внесении изменений в Требования по обеспечению безопасности значимых объектов КИИ, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239»

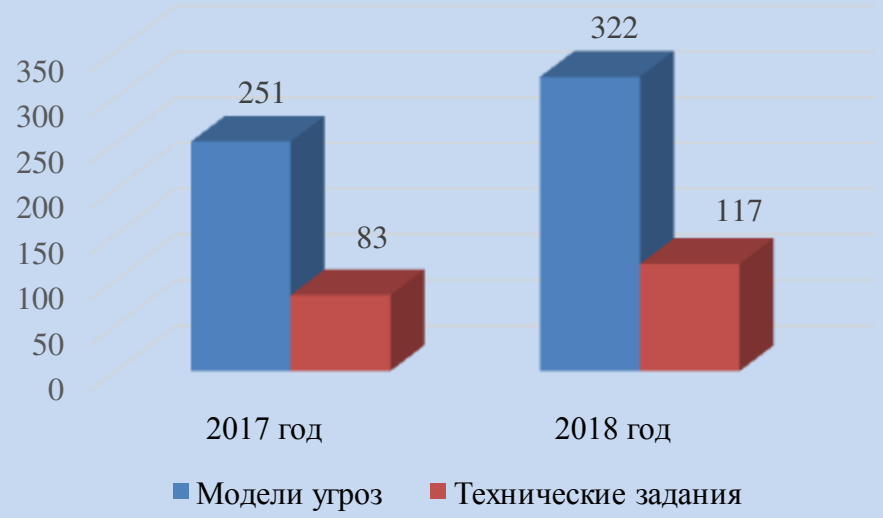
Приказ ФСТЭК России «О внесении изменений в Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235»

СОГЛАСОВАНИЕ ДОКУМЕНТАЦИИ НА СОЗДАНИЕ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации

утверждены постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676
(в редакции постановления Правительства Российской Федерации от 11 мая 2017 г. № 555)

Количество рассмотренных моделей угроз и технических заданий



В 2018 году рассмотрено:
более 300 моделей угроз
более 100 технических заданий

Количество рассмотренных документов в 2018 году увеличилось в 1,2 раза

Около 30% документов возвращаются на доработку

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ СЕРТИФИКАЦИИ ФСТЭК РОССИИ

Положение о системе сертификации средств защиты информации

утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55
зарегистрирован Минюстом России 11 мая 2018 г. № 51063, вступил в силу с 1 августа 2018 г.

Увеличение срока действия сертификата соответствия до 5 лет

Исключение необходимости продления сертификата пользователями средств защиты информации

Детализация процедур сертификации, установление сроков осуществления процедур сертификации

Определение порядка внесения изменений в сертифицированные СЗИ

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

утверждены приказом ФСТЭК России от 30 июля 2018 г. № 131
приказ зарегистрирован Минюстом России 14 ноября 2018 г. № 52686

Требования к разработке средства

Требования к проведению испытаний средства

Требования к поддержке безопасности средства

СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ И НДВ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

утверждены приказом ФСТЭК России от 30 июля 2018 г. № 131

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

утверждена ФСТЭК России 11 февраля 2019 г.

Применяются при проведении сертификационных испытаний с 1 мая 2019 г.

Этап 1. Подготовка к проведению исследований

- Анализ документации и других источников, содержащих сведения об объекте оценки
- Подготовка исследовательского стенда

Этап 2. Проведение исследований

- Экспертный анализ объекта оценки
- Статический анализ объекта оценки
- Динамический анализ объекта оценки
- Ручной анализ объекта оценки

Этап 3. Оформление результатов исследований

- Разработка протоколов проведения исследований объекта оценки
- Разработка заключения о результатах исследований объекта оценки

СОВЕРШЕНСТВОВАНИЕ ДЕЯТЕЛЬНОСТИ ТК 362

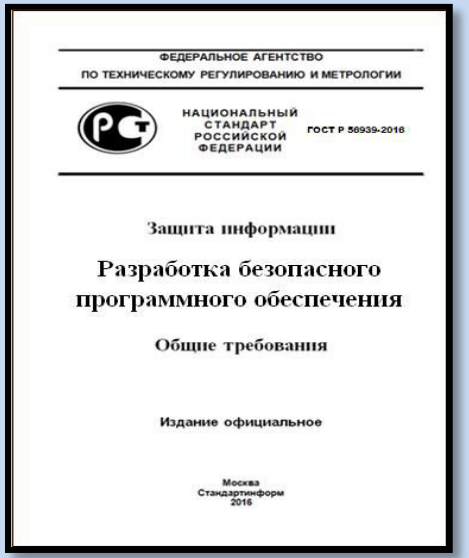
Структура технического комитета по стандартизации «Защита информации» (ТК 362)

ПК 1
Общеметодологический

ПК 2
Защита информации на объектах информатизации объектах критической информационной инфраструктуры

ПК 3
Средства и методы защиты информации

ПК 4
Разработка безопасного программного обеспечения


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56939-2016

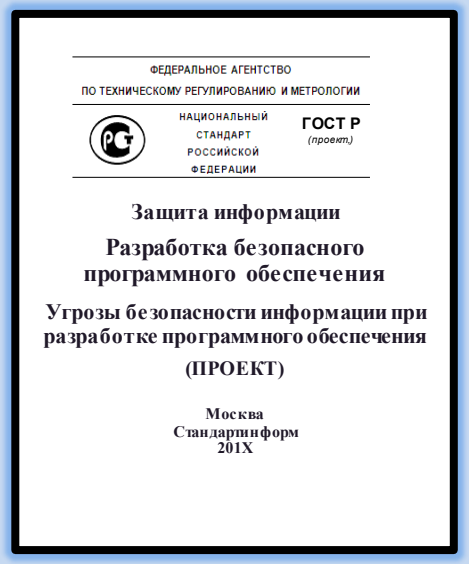
Защита информации

Разработка безопасного программного обеспечения

Общие требования

Издание официальное

Москва
Стандартинформ
2016


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р (проект)

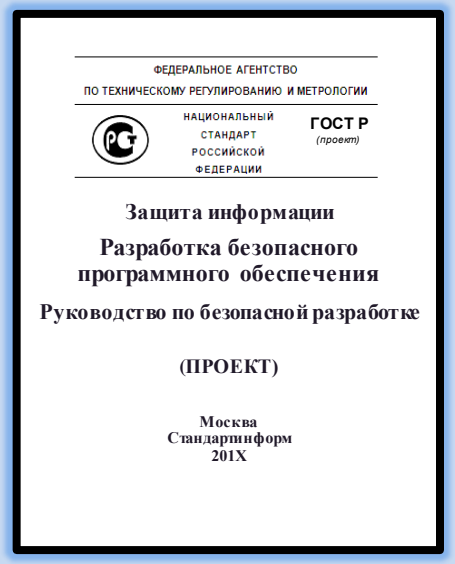
Защита информации

Разработка безопасного программного обеспечения

Угрозы безопасности информации при разработке программного обеспечения

(ПРОЕКТ)

Москва
Стандартинформ
201X


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р (проект)

Защита информации

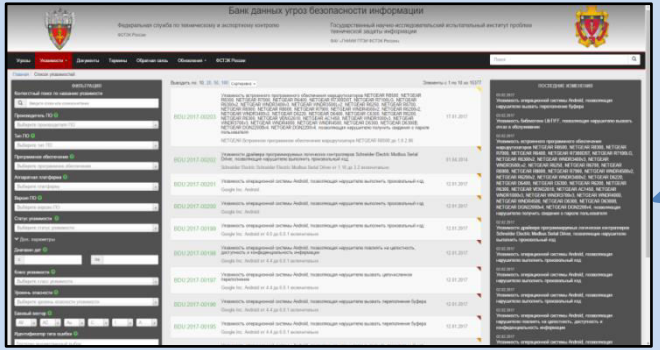
Разработка безопасного программного обеспечения

Руководство по безопасной разработке

(ПРОЕКТ)

Москва
Стандартинформ
201X

СОВЕРШЕНСТВОВАНИЕ БАНКА ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ



По состоянию на февраль 2019 г.
Банк данных содержит:

- сведения о **213** угрозах безопасности информации;
- сведения о **более 20 000** уязвимостей

Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России

утвержден ФСТЭК России 26 июня 2018 г.

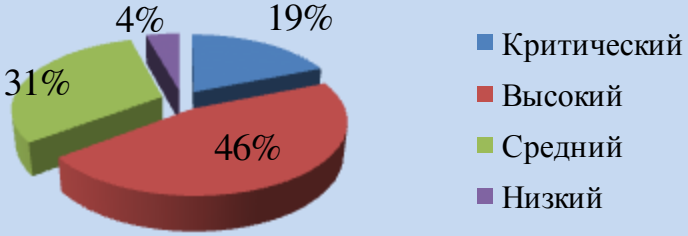
Условия раскрытие информации об уязвимостях

Информация об уязвимости и мерах по ее устранению получена от разработчика

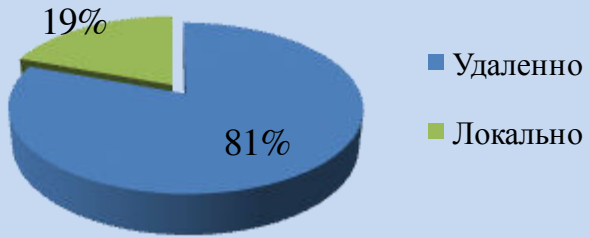
Разработчик не реагирует на уведомления об обнаруженных уязвимостях

Разработчик уклоняется от устранения уязвимостей и не принимает меры по их устранению

Уровень опасности уязвимостей:



Реализация уязвимостей:



Направления совершенствования технической защиты информации и обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Заместитель директора ФСТЭК России
Лютиков Виталий Сергеевич