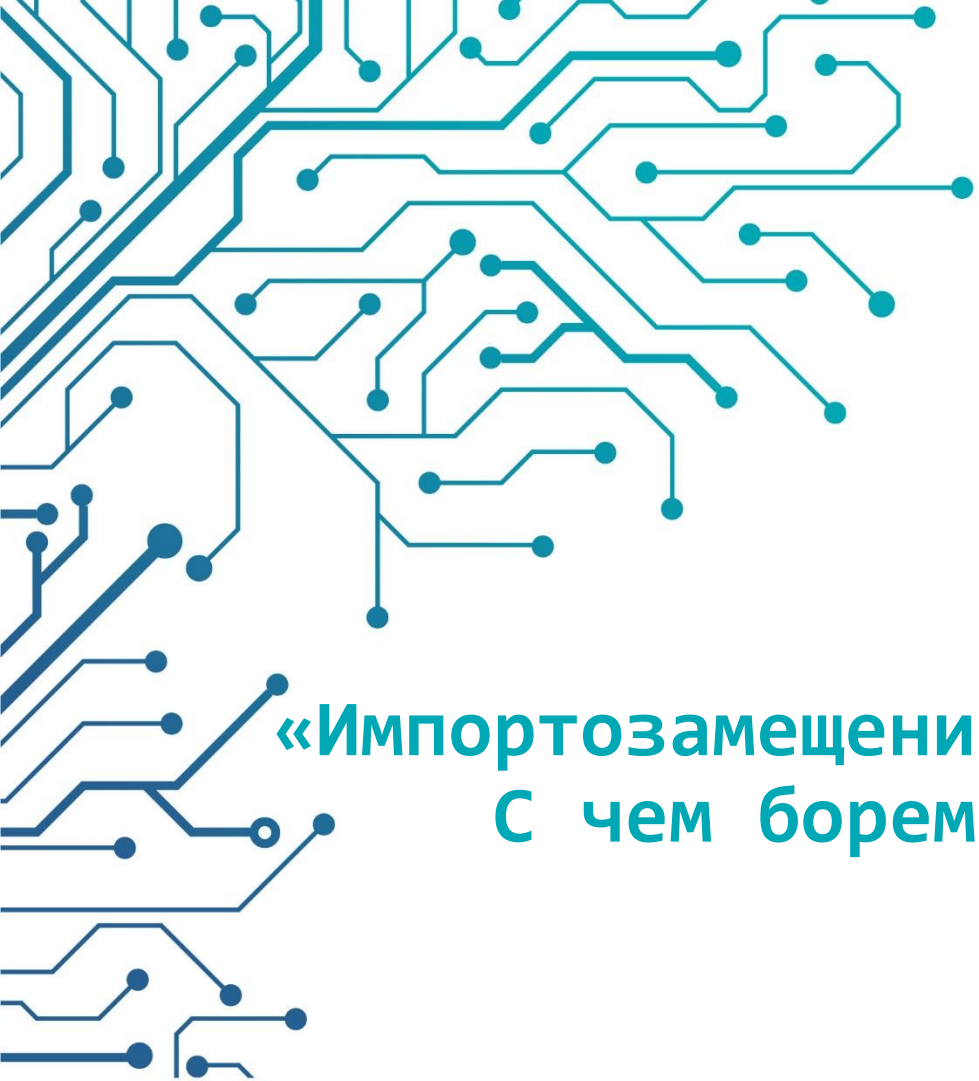


Конференция «Электронный регион: территория безопасности»

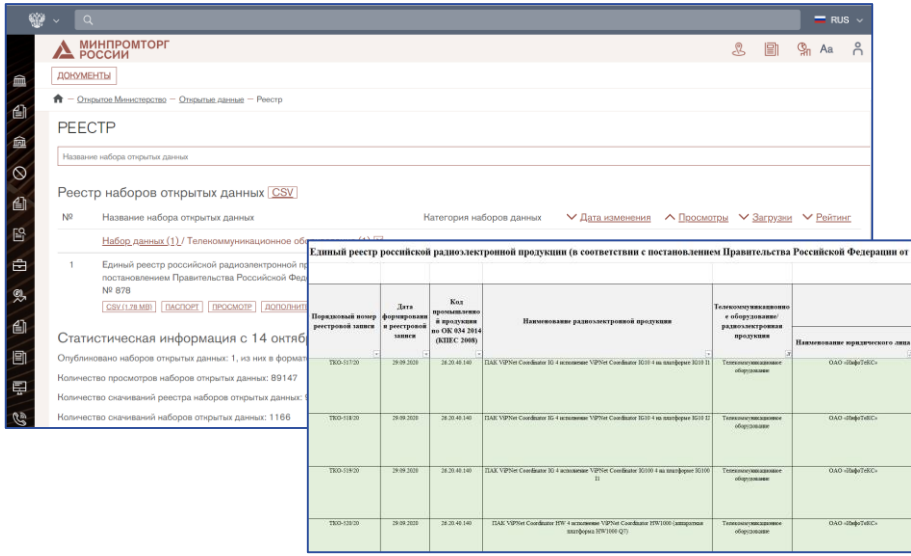
«Импортозамещение и другие тренды ИБ. С чем боремся, к чему готовимся»

Акимов Сергей Леонидович

Импортозамещение. Новый виток

Правительство РФ, Минпромторг России

- Постановлением правительства № 878 от 10 июля 2019 года введен Перечень радиоэлектронной продукции, происходящей из иностранных государств, в отношении которой с 1 сентября 2019 года устанавливаются ограничения для целей осуществления закупок для обеспечения государственных и муниципальных нужд.
- Постановлением Правительства РФ от 21.12.2019 № 1746 установлен запрет на закупку отдельных видов товаров иностранного производства.



(https://gisp.gov.ru/documents/10546664/)

Перечень включает:

Оборудование компьютерное, электронное и оптическое *(и серверы общего назначения и АРМы и терминалы)*, в том числе:

- СЗИ
- Информационные и телекоммуникационные системы, защищенные с использованием СЗИ

Результат – государственные заказчики должны включать в свои закупочные процедуры пункт о наличии закупаемой продукции в Едином реестре российской радиоэлектронной продукции (далее - РРП).

Импортозамещение. Новый виток

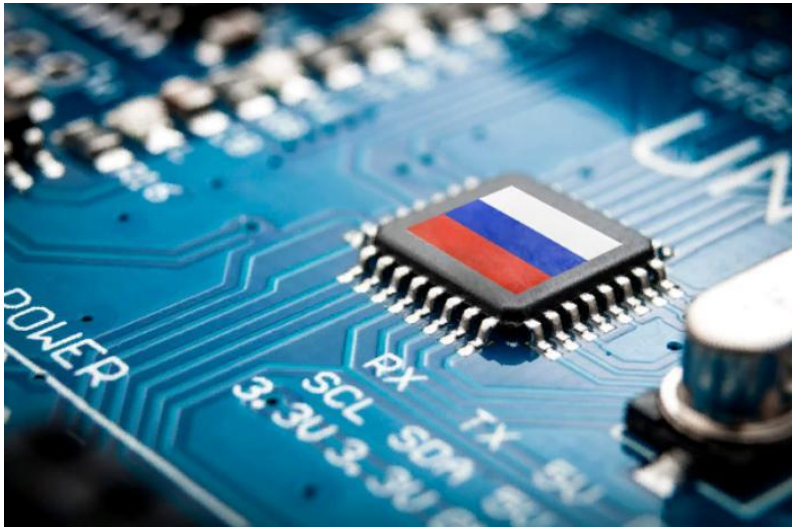
Минцифры

Подготовило проект Указа Президента Российской Федерации «О мерах экономического характера по обеспечению технологической независимости и безопасности объектов критической информационной инфраструктуры».

Проектом документа предполагается переход субъектов КИИ на преимущественное использование российского:

1. Программного обеспечения до 1 января 2024 г.
2. Оборудования до 1 января 2025 г.

Сокращение сроков импортозамещения. Для субъектов КИИ – до 01.01.2023



ФСТЭК России

Подготовила проект приказа О внесении изменений в Положение о системе сертификации средств защиты информации, утвержденное приказом Федеральной службы по техническому и экспортному контролю от 3 апреля 2018 г. № 55

Защита критической информационной инфраструктуры

Срез по объектам КИИ

Иностранное оборудование и ПО

Полное или частичное импортозамещение

Средства ИБ на объектах КИИ гос.органов

Иностранное оборудование и ПО

Российское оборудование и ПО

Стандартизация подходов к криптографической защите промышленных протоколов

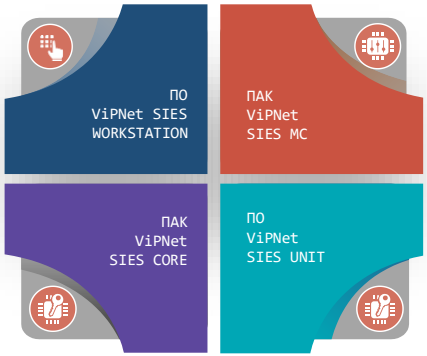
Разработан ТК 26 «Криптографическая защита информации»

CRISP – первый в России специализированный протокол криптозащиты для индустриальных систем

Р 1323565.1.029–2019 «Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем» (CRISP 1.0) – введены в действие 01.09.2020

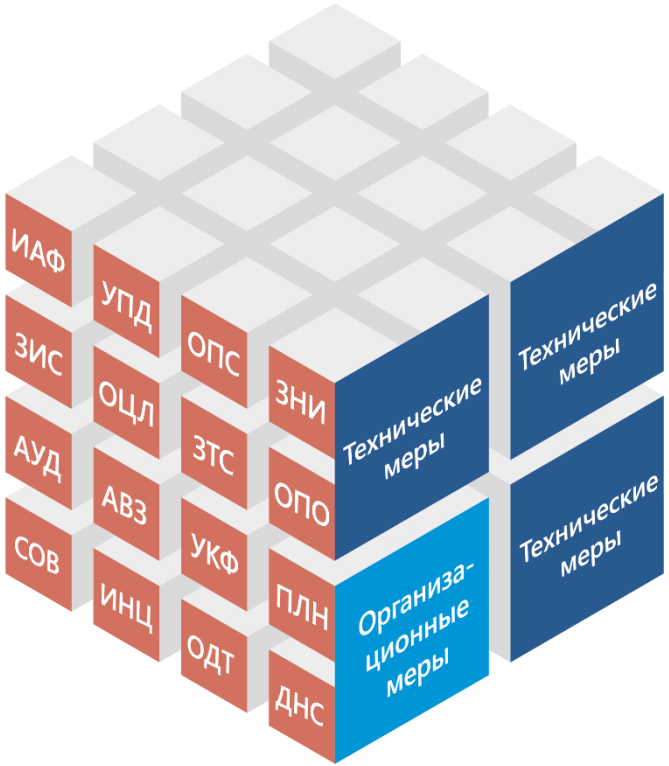
Кстати: Р1323565.1.034-2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня» (IPlir) – введены в действие 01.04.2021

Решение ViPNet SIES



Решение ViPNet Coordinator IG

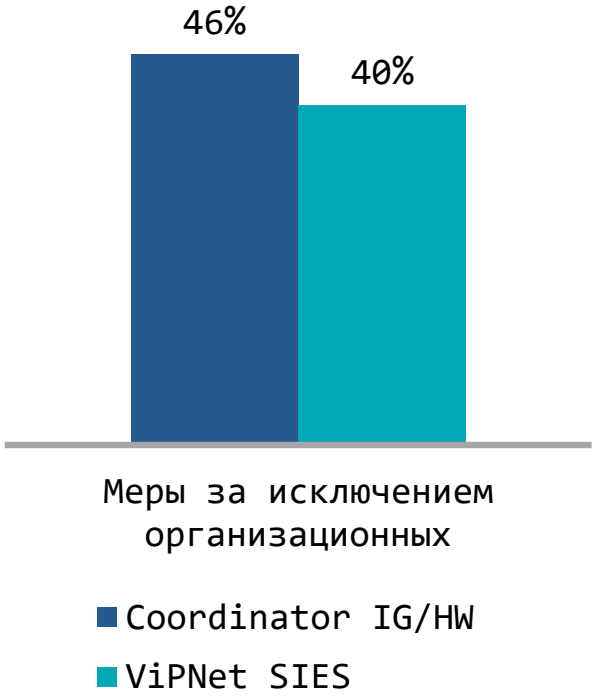
Состав мер по защите объектов КИИ согласно Приказу №239 ФСТЭК России



- Идентификация и аутентификация (ИАФ)
- Управление доступом (УПД)
- Ограничение программной среды (ОПС)
- Защита машинных носителей информации (ЗНИ)
- Аудит безопасности (АУД)
- Антивирусная защита (АВЗ)
- Предотвращение вторжений (компьютерных атак) (СОВ)
- Обеспечение целостности (ОЦЛ)
- Обеспечение доступности (ОДТ)
- Защита технических средств и систем (ЗТС)
- Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
- Планирование мероприятий по обеспечению безопасности (ПЛН)
- Управление конфигурацией (УКФ)
- Управление обновлениями программного обеспечения (ОПО)
- Реагирование на инциденты информационной безопасности (ИНЦ)
- Обеспечение действий в нештатных ситуациях (ДНС)
- Информирование и обучение персонала (ИПО)

всего 152 меры

Соответствие мерам Приказа ФСТЭК России №239



Комбинированный подход

ФСТЭК России. Безопасная разработка. Обеспечение требований доверия

ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

30.07.2018 г. Приказом ФСТЭК №131 утверждены Требования доверия.

С 1 января 2020 г. действие сертификатов на СЗИ в отношении которых не проведена оценка соответствия Требованиям доверия может быть приостановлено.

02.06.2020 Приказом ФСТЭК России №76 утверждена НОВАЯ РЕДАКЦИЯ Требований доверия

НОВЫЕ Требования доверия вступили в силу с 1 января 2021 г.
Включены требования об использовании отечественных аппаратных платформ и элементной базы:

с 1 января 2022 г.:
- Сведения об АП СЗИ должны быть включены в РРП
- Сведения об АП СВТ, являющегося СФ СЗИ, должны быть включены в РРП

с 1 января 2024 г.:
- Сведения о процессорах или микросхемах, выполняющих функции процессоров (микроконтроллеры), элементах памяти, сетевых картах, графических адаптерах АП СВТ, являющегося СФ СЗИ, должны быть включены в РРП

с 1 января 2028 г.:
- Сведения о процессорах или микросхемах, выполняющих функции процессоров (микроконтроллеры), элементах памяти, сетевых картах, графических адаптерах АП СЗИ должны быть включены в РРП

25.12.2020 ФСТЭК России утверждена новая Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении.

ЦБ. Новые Положения/Новые требования

2019 год:

- 683-П Требования для кредитных организаций (противодействие осуществлению ПДС без согласия клиента)
- 684-П Требования для не кредитных организаций (противодействие осуществлению незаконных финансовых операций)

2020 год:

- 716-П Требования к системе управления операционными рисками в кредитной организации и банковской группе
- 719-П Требования по обеспечению защиты информации при осуществлении переводов денежных средств
- 742-П Требования по защите информации оператором финансовой платформы
- 747-П Требования к защите информации в платежной системе Банка России

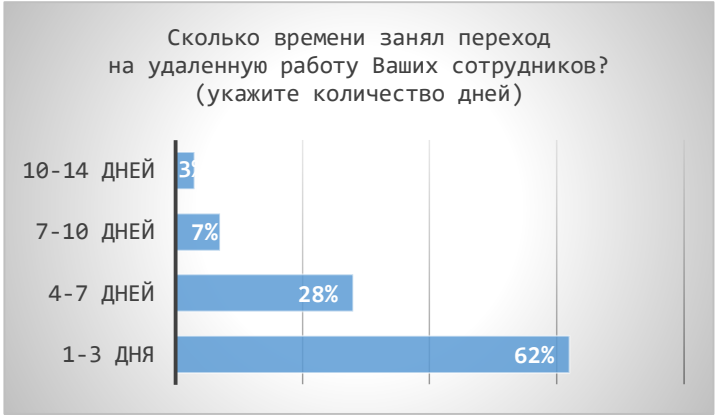
и др…

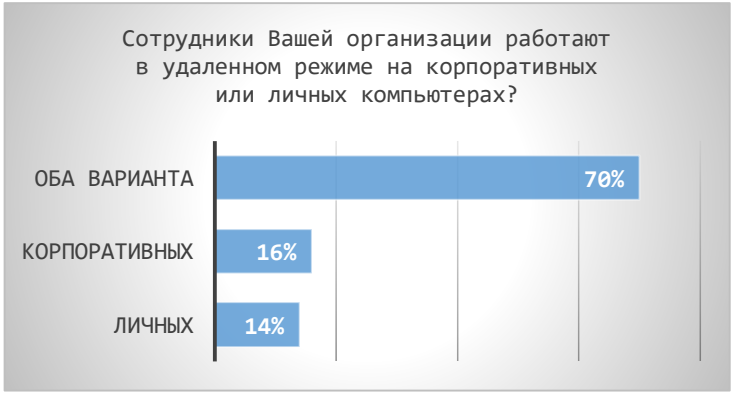
При использовании СКЗИ для защиты банковской и платежной информации Положения учитывают требования о соблюдении норм ФЗ «Об электронной подписи» и ПКЗ-2005.

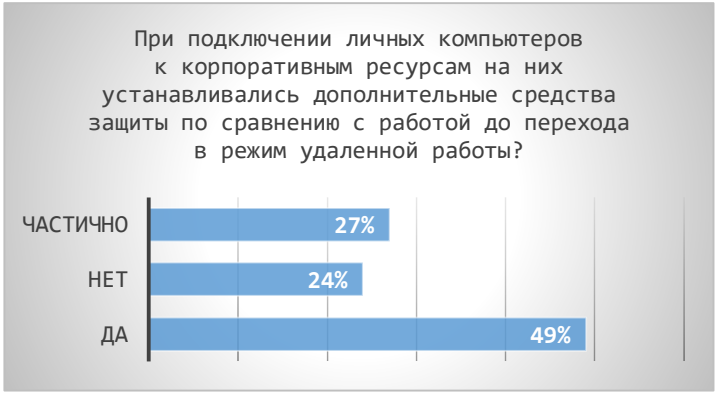
Должен быть осуществлен поэтапный переход участников платежного рынка на использование только отечественных СКЗИ до 2031 года.

COVID. Вынужденная удаленная работа

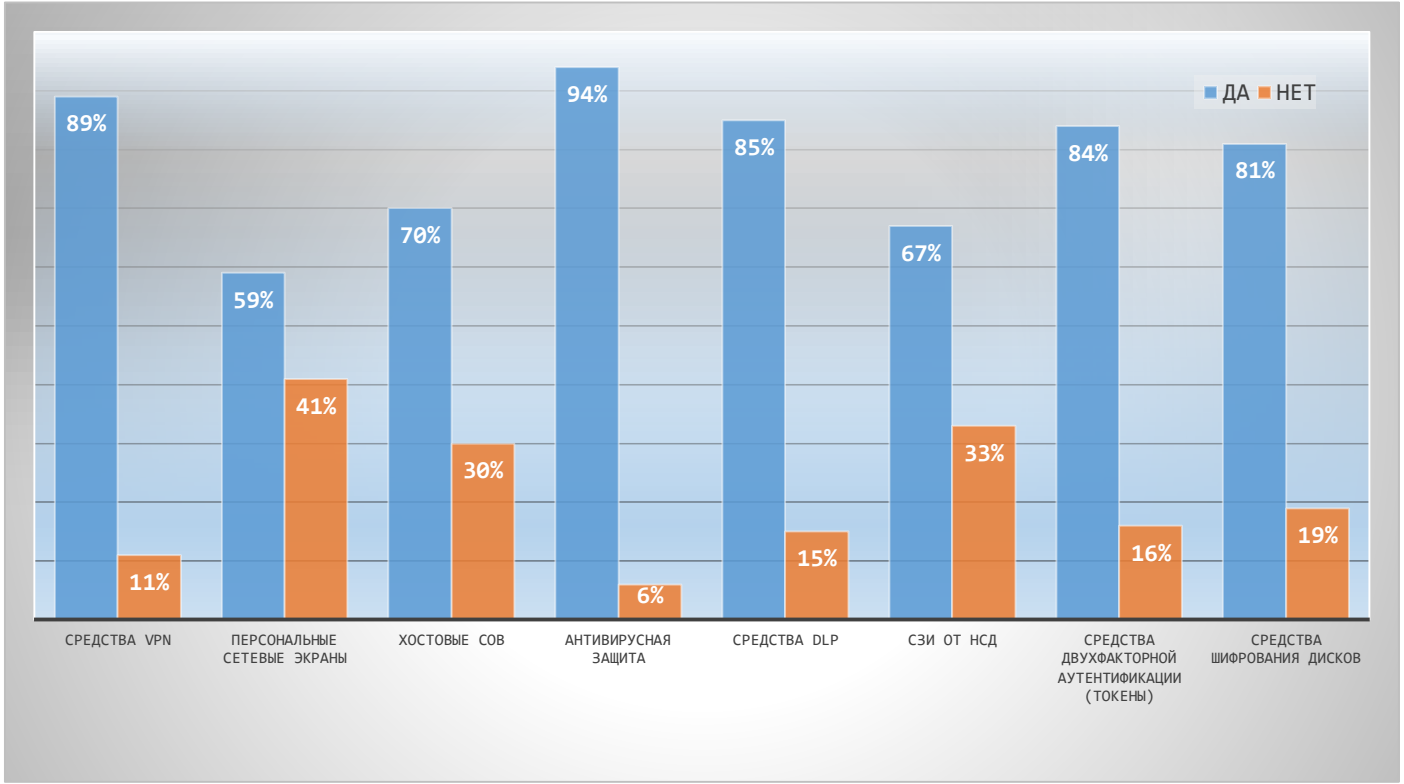
Опрос по организации удаленной работы
(материалы АО «ИнфоТеКС»)



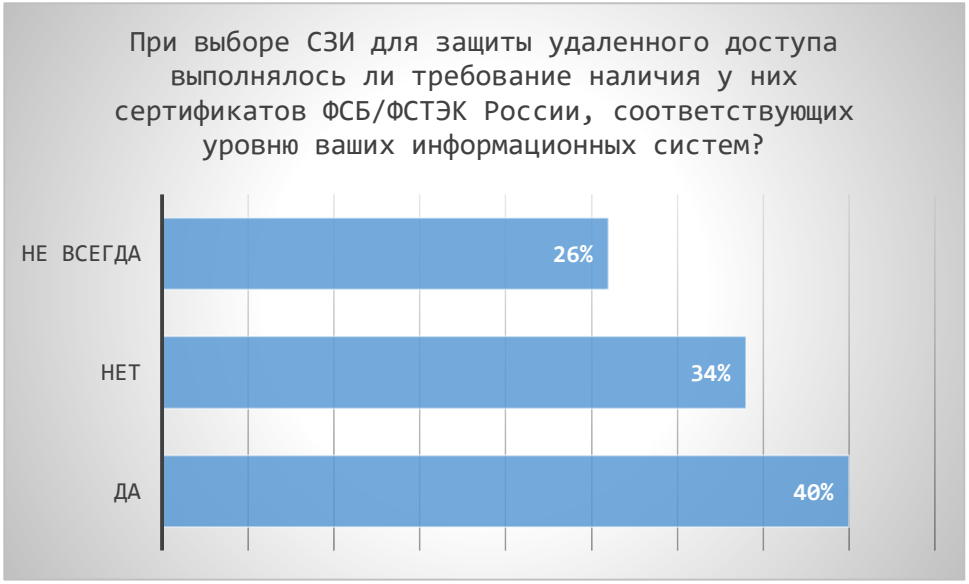




Средства защиты при удаленном подключении



Сертифицированные СЗИ для удаленного доступа

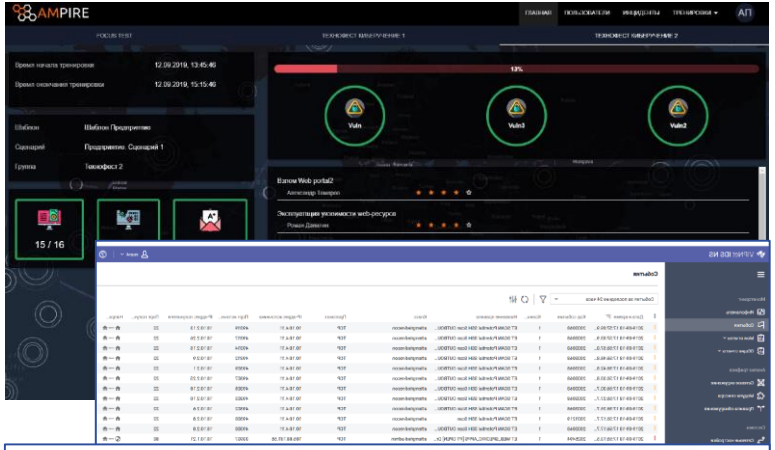


Киберполигон

Учебно-тренировочная платформа AMPIRE

Задачи:

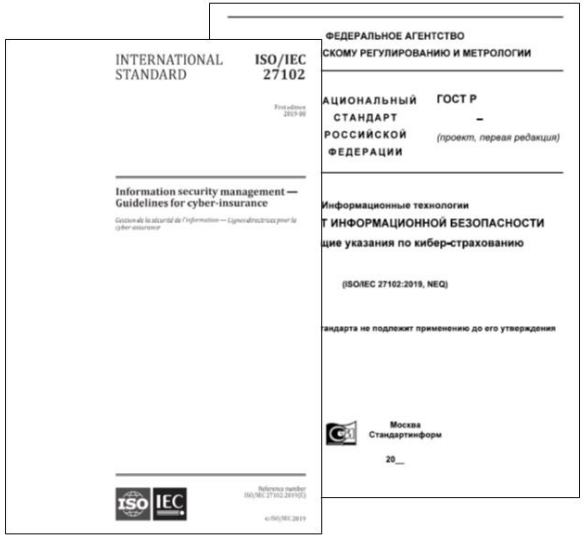
- отработка навыков выявления компьютерных атак
- отработка навыков расследования инцидентов ИБ
- отработка навыков оценки защищенности элементов информационных сетей
- отработка взаимодействия между подразделениями
- отработка методических рекомендаций по нейтрализации компьютерных атак
- отработка превентивных мер по предупреждению компьютерных атак и инцидентов



Страхование киберрисков

Зарубежные тенденции:

- Концепции страхования киберрисков как инструмента управления рисками сформированы еще в 1990-е, направление имеет последовательное развитие
- К 2015 году услуги по страхования киберрисков предлагают уже более 80 страховщиков во всем мире
- Эксперты прогнозируют десятикратный рост полученных страховых премий в 2025 году по сравнению с 2015 годом – с 2 млрд. долларов США до 20



Наша действительность:

- Дефицит методической базы технического плана и практики ее использования в РФ
- Информация об услугах страхования киберрисков имеет в основном рекламный характер – оценка емкости рынка
- Услуги по страхованию киберрисков по факту выливаются в предложения об имущественном страховании – как следствие дефицита методической базы технического плана

Резюме

- Государство выдвигает глобальные инициативы в части импортозамещения. Многие из них реализуются, но далеко не все
- Промышленность продолжает выживать, искать новые формы
- Направление КИИ подошло к периоду реальных внедрений
- Как и другие компании, АО «ИнфоТеКС» адаптируется к заданным трендам. Многие решения не только остались востребованными, но и приобрели решающее значение для безопасного и быстрого функционирования организации в условиях пандемии

Спасибо за внимание!

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow