МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

по профессии

«Техник по защите информации»

с учётом стандарта Ворлдскиллс Россия по компетенции

«Корпоративная защита от внутренних угроз информационной безопасности»

а к а д е м и я

2018 г.

Программа повышения квалификации преподавателей
(мастеров производственного обучения)
«Практика и методика подготовки кадров по профессии
(специальности) «Техник по защите информации» с учетом
стандарта Ворлдскиллс Россия по компетенции

«Корпоративная защита от внутренних угроз информационной безопасности»

Рабочая тетрадь слушателя

версия 1.0

А.В. Сергеев

Глава 1. Ознакомление с WSI и Ворлдскиллс Россия

Ознакомление с WSI и Ворлдскиллс Россия

- WorldSkills – это международное некоммерческое Движение, целью которого является повышение престижа рабочих профессий и развитие профессионального образования путем гармонизации лучших практик и профессиональных стандартов во всем мире посредством организации и проведения конкурсов по профессиональному мастерству, как в каждой из 80+ стран-членов Движения WSI, так в мире в целом.
- Официальным представителем Российской Федерации в WorldSkills International и оператором конкурсов по профессиональному мастерству по стандартам WorldSkills на территории нашей страны является Союз «Агентство развития профессиональных сообществ и рабочих кадров «Ворлдскиллс Россия», учреждённый Правительством Российской Федерации совместно с Агентством стратегических инициатив.
- Полномочия учредителей союза от имени Российской Федерации осуществляют Минобрнауки России и Минтруд России

Министерство образования и науки Российской Федерации

МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ РФ

АГЕНТСТВО СТРАТЕГИЧЕСКИХ ИНИЦИАТИВ

Ознакомление с WSI и Ворлдскиллс Россия

WorldSkills действительно дает возможности:

- **Экспертам** – осваивать новые методы обучения и технологии, участвовать в формировании стандартов профессий;
- **Государству** – измерять и сравнивать уровень навыков специалистов и учащихся, участвующих в чемпионатах по стандартам WorldSkills по всей стране.
- **Работодателям** – подбирать для себя персонал на этапе получения учащимися профессионального образования.
- **Учебным заведениям** – обновление материальной базы, повышение качества образование, прямая связь с индустрией.
- **Учащимся** – изучать современные технологии и лучшие мировые практики, участвовать в региональных, окружных, национальных и международных чемпионатах, получать от работодателей предложения о трудоустройстве.

Союз «Молодые профессионалы «WorldSkills Russia»

- Региональная сеть в СПО по всей стране
  - вовлечены все регионы РФ
  - 100+ ВУЗов
  - В 2017 году 14 000 выпускников колледжей и техникумов впервые сдали демонстрационный экзамен по стандартам WorldSkills Russia
- Экспертное сообщество
- Работа над улучшением профстандартов
- Повышение квалификации специалистов
- Работа над гармонизацией стандартов Worldskills и образовательных стандартов

РЕГИОНАЛЬНЫЙ ЧЕМПИОНАТ “МОЛОДЫЕ ПРОФЕССИОНАЛЫ”

Проводятся в регионах РФ
Организаторы: органы исполнительной власти региона, РКЦ, образовательные организации работодатели

ОТБОРОЧНЫЕ СОРЕВНОВАНИЯ ПО СФЕРАМ КОМПЕТЕНЦИЙ

Проводятся по сферам компетенций (Творчество и дизайн, Обслуживание гражданского транспорта, Сфера услуг, Специалисты промышленного производства, Специалисты IT, Строительная сфера)

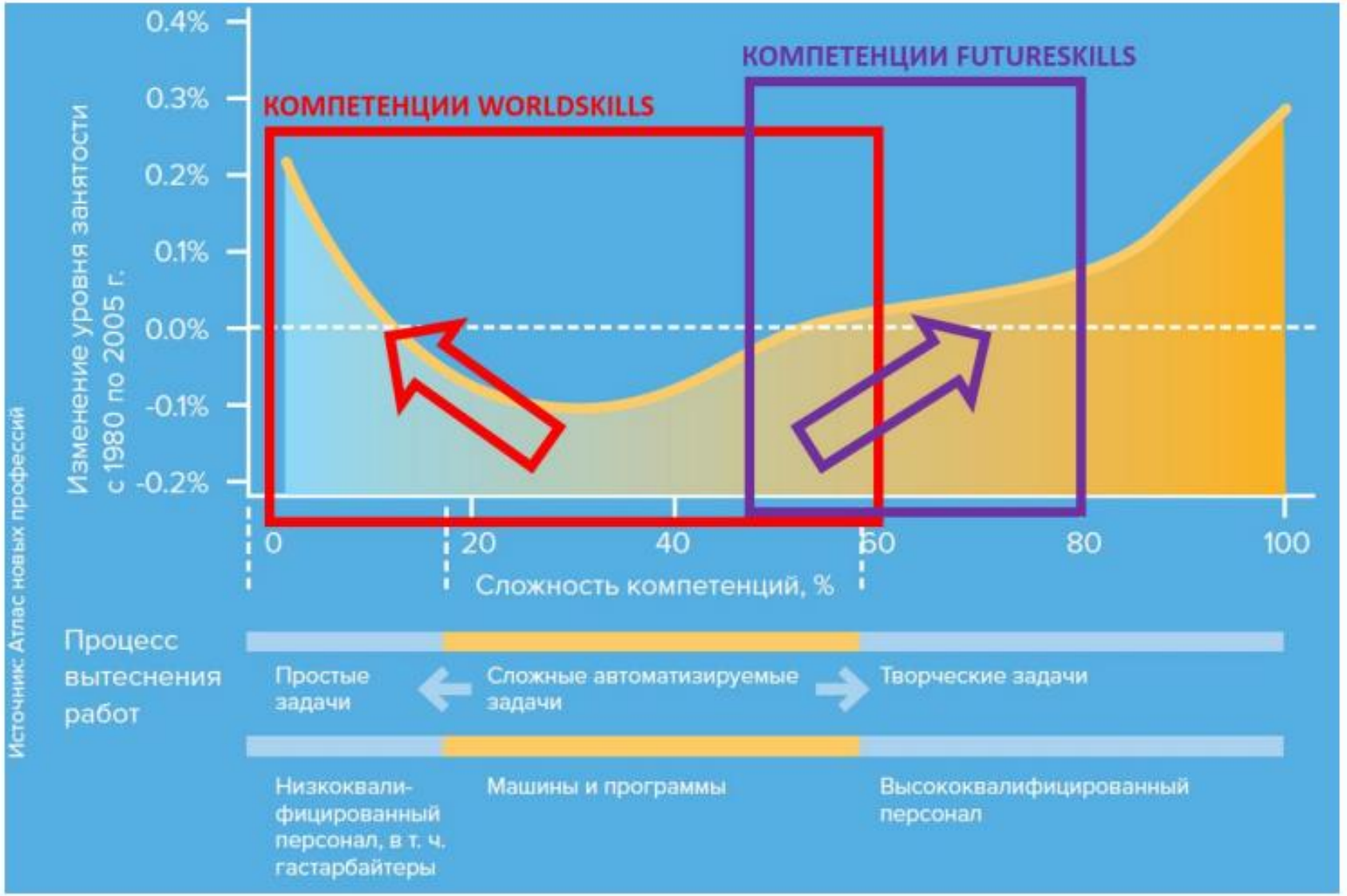
НАЦИОНАЛЬНЫЙ ЧЕМПИОНАТ “МОЛОДЫЕ ПРОФЕССИОНАЛЫ”

Самые масштабные соревнования профессионального мастерства по стандартам WorldSkills в котором принимают участие 84 региона РФ

МИРОВОЙ ЧЕМПИОНАТ WORLDSKILLS COMPETITION

Соревнования в котором выступают конкурсанты из стран-участниц движения WorldSkills International.
В 2019 мировой чемпионат примет г. Казань

Опережающая подготовка кадров и развитие профессий



ГУАП: создание компетенций вместе с лидерами индустрии

- **Интернет вещей**
  - PTC (ThingsWorx),
    Intel → National Instruments, MGBot
- **Организация эффективного производства**
  - Fanuc

- **Корпоративная защита от внутренних угроз ИБ**
  - Infowatch
- **Разработка микросервисов для корпоративных PaaS**
  - DellEMC

+ Инженерия космических систем, Мобильная робототехника,
+ Программные решения для бизнеса

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

DELL

ptc

FANUC ROBOTICS

2016
Интернет вещей

2017
- Организация эффективного производства
- Корпоративная защита от внутренних угроз ИБ

2018
Разработка микросервисов для корпоративных PaaS

WorldSkills International, 2019 (Kazan)

EuroSkills 2022 (St. Petersburg)

___ ___ 2018

Глава 2. Современные технологии в профессиональной сфере деятельности по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

Корпоративная защита от внутренних угроз информационной безопасности

- Комплекс профессиональных мер и действий, связанных с обеспечением защиты предприятия от внутренних угроз информационной безопасности.
- Ключевые навыки:
  - способность выявлять и оценить риски, связанные с внутренними угрозами информационной безопасности предприятия;
  - способность определять каналы передачи информации, подлежащие защите средствами автоматизированных систем контроля информационных потоков организации;
  - способность проводить аудит информационных активов предприятия и бизнес-контекст их обработки в ИС предприятия в соответствии с принятыми процессами и процедурами;
  - способность разрабатывать и внедрять политики внутренней информационной безопасности;
  - способность создания нормативно-правовой основы для внедрения и использования систем автоматизированного контроля информационных потоков класса DLP и проведения служебных расследований инцидентов внутренней информационной безопасности
  - способность администрировать и использовать в профессиональной деятельности системы контроля информационных потоков организации, проводить расследование инцидентов информационной безопасности и готовить соответствующие отчеты.

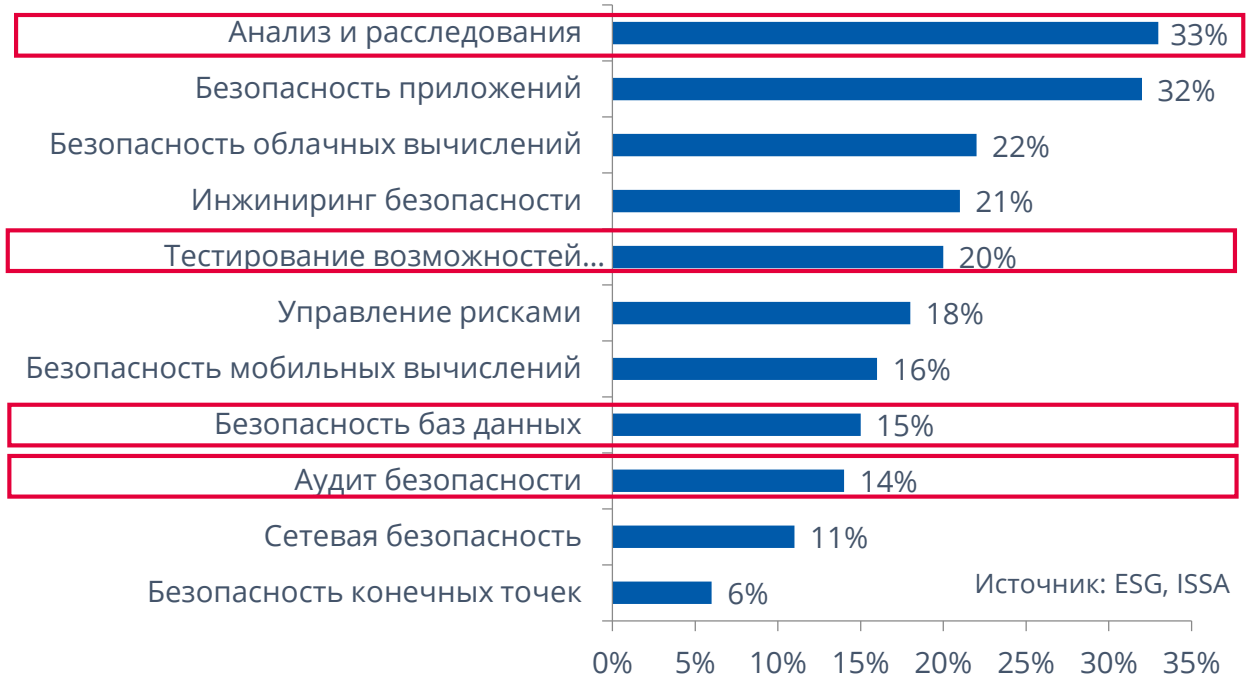
___ ___ 2018

___ ___ 2018

___ ___ 2018

Обоснование потребности в компетенции

Каких навыков информационной безопасности не хватает больше всего?
(Опрос 437 специалистов, 2016, мир)



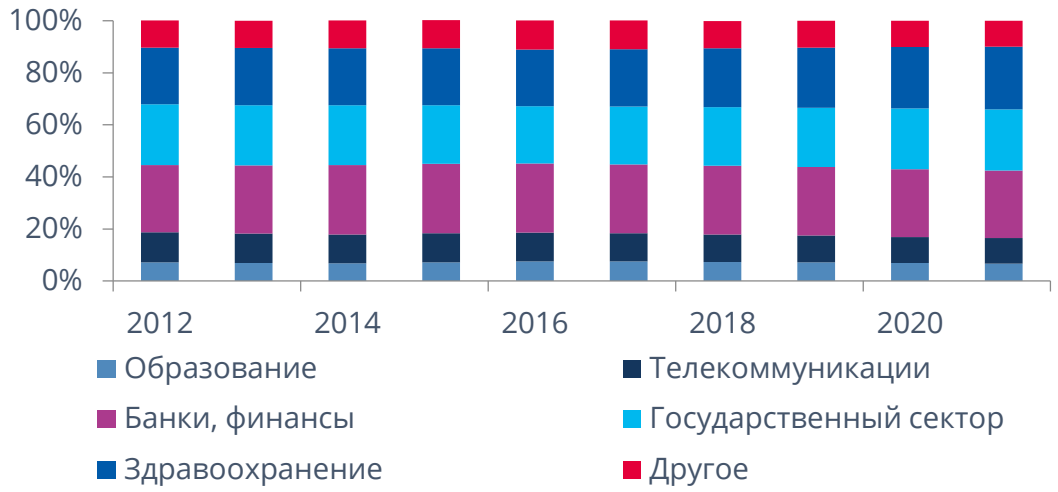
Сферы, в которых конфиденциальная информация защищена законодательно (Россия)

- Медицина
- Наука и изобретательство
- Юриспруденция
- Силовые структуры
- Банки и финансы

45% компаний в России говорят о **дефиците специалистов** по информационной безопасности (Kaspersky Lab, 2016 г.)

1,8 млн специалистов по информационной безопасности **не будет хватать** к 2022 г. (GISWS)

Прогноз продаж ПО и услуг контентной безопасности по отраслям, 2012-2021



___ ___ 2018

Контроль информации = контроль бизнеса

ПО/ПАК информационной безопасности

- DLP-системы
- SIEM
- IRM
- И другие

Корпоративное ПО

- ERP
- CRM
- IP-телефония
- И другие

Задача ИБ-специалиста – контролировать все потоки информации

Задача ИБ-специалиста – контролировать все потоки информации

___ ___ 2018

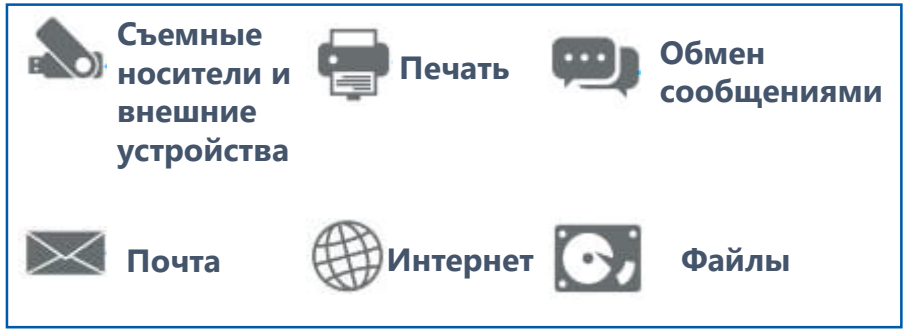
Система корпоративной защиты от внутренних угроз информационной безопасности

Методы защиты корпоративной информационной среды

- Система управления идентификацией и доступом пользователей (Identity and Access Management (IAM))
- Система управления событиями информационной безопасности (Security Information Event Management (SIEM))
- Средства предотвращения потери данных (Data Loss/Leak Prevention (DLP)):
  - контроль рабочих станций сотрудников;
  - контроль трафика корпоративной сети;
  - контроль сетевых хранилищ информации

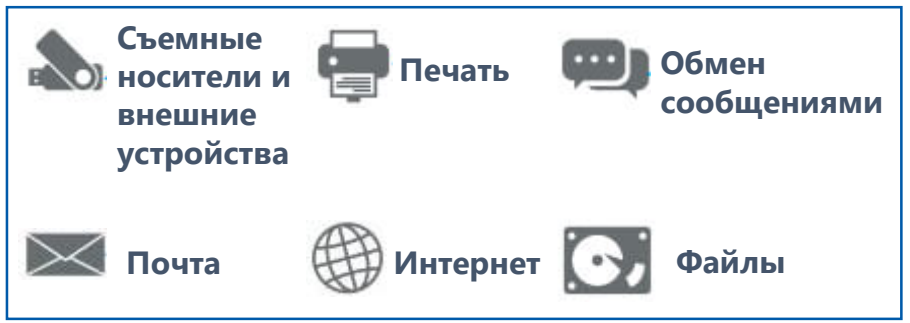
Защищаемые элементы корпоративной информационной среды

Рабочие станции сотрудников

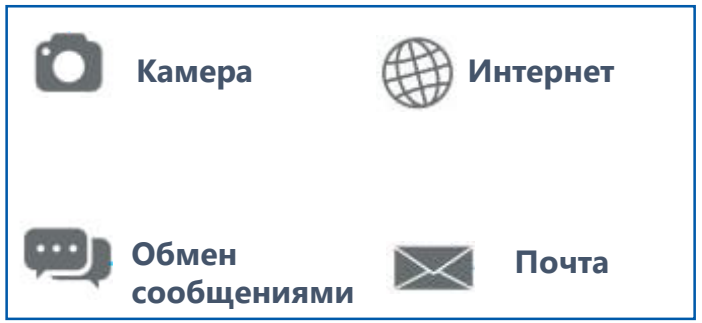


Сетевые хранилища

Удаленно работающие сотрудники



Мобильные устройства

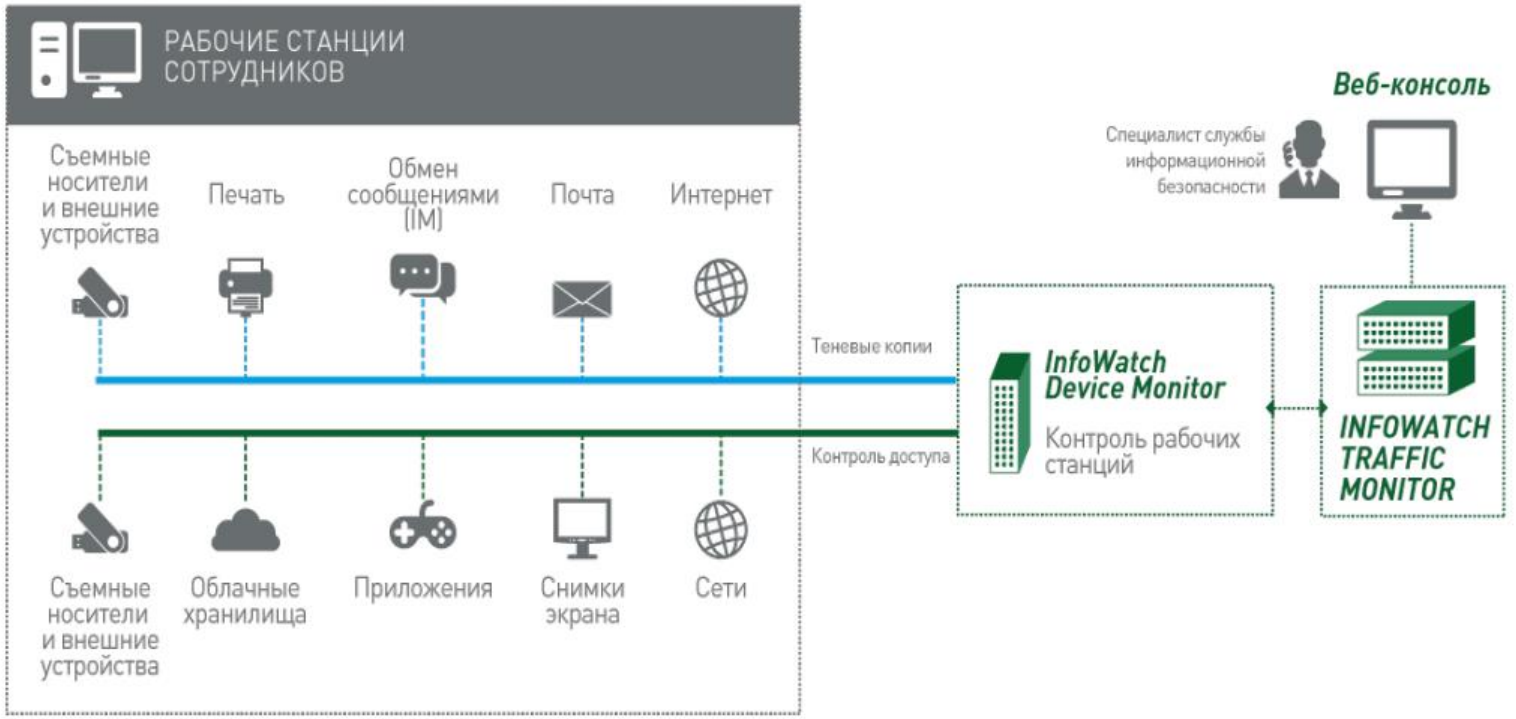


___ ___ 2018

DLP как ядро системы корпоративной безопасности

___ ___ 2018

Архитектура DLP-системы



- DLP-системы работают с информацией и событиями
- ИТ-системы генерируют информацию и события внутри корпоративной сети

Новые требования к DLP-системам:

- Обмен данными и интеграция с другими ИТ системами организации
- Упрощение процесса интеграции DLP в инфраструктуру
- Глубокий анализ данных

___ ___ 2018

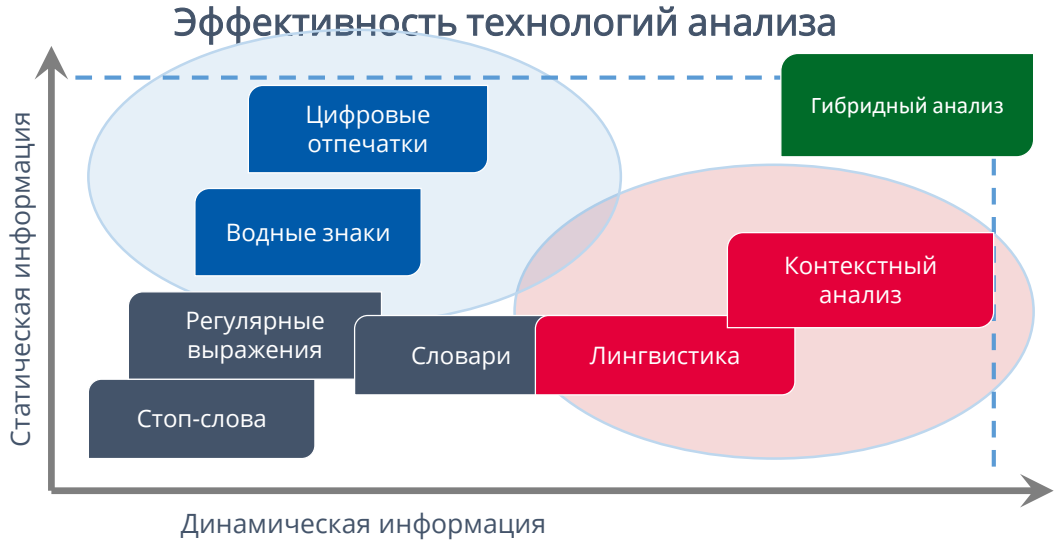
___ ___ 2018

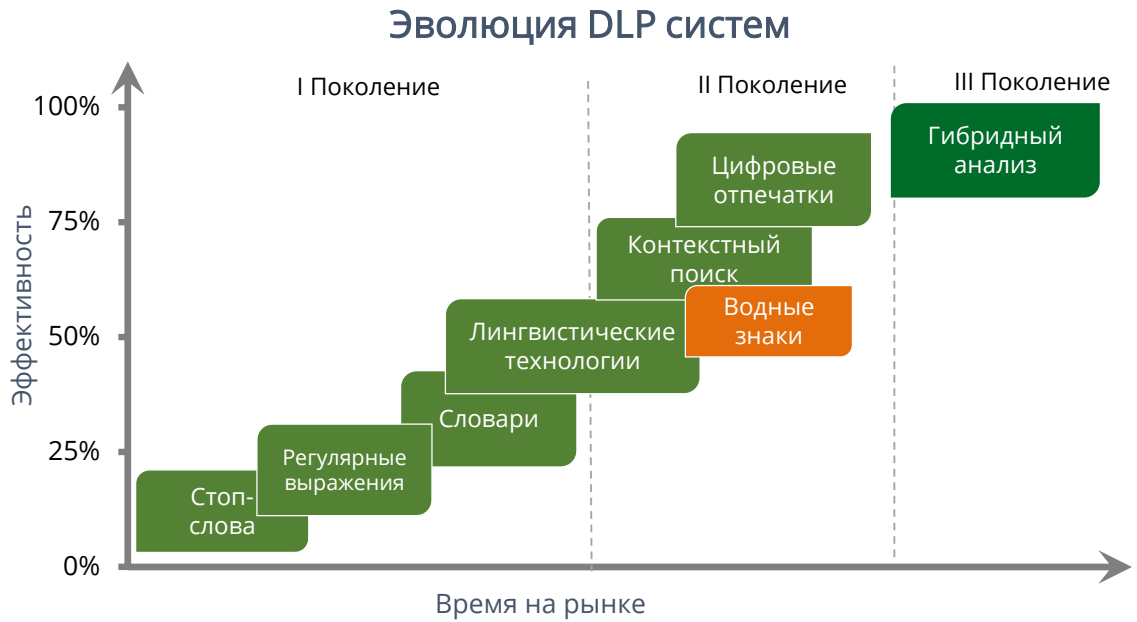
Глава 3. Стандарт компетенции WSSS «Корпоративная защита от внутренних угроз информационной безопасности»

Корпоративная защита от внутренних угроз ИБ

Факторы изменений DLP технологий:

- Цифровая трансформация бизнеса набирает обороты, бумажные документы отходят на второй план
- У предприятий появляется все больше информационных активов различного формата, которым необходимо обеспечить всестороннюю защиту;
- На предприятиях применяется **множество разнотипных устройств** и каналов связи, и их число постоянно растет увеличивается
- В бизнес-процессы внедряются **облачные и мобильные технологии**, что требует модификации систем защиты;
- Приоритет смещается в сторону **предотвращения инцидентов**, а не реагирования на них, например, в сторону фокусировки на рисках социального инжиниринга;
- В технологии защиты внедряются **искусственный интеллект и машинное обучение**
- Самым слабым звеном в обеспечении информационной безопасности становится становится пользователь с доверенным доступом





Источник: Infowatch

___ ___ 2018

Чемпионаты WorldSkills по компетенции

- **2017**
  - Пилотный чемпионат СПбГУАП – 5 комад
  - HiTech (Екатеринбург) – 3 команды
  - Digital Skills (Иннополис) – 6 команд из 5 регионов
- **2018**
  - Пилотный чемпионат СПО «Мастера Москвы» – 14 команд
  - Чемпионаты ВУЗов – 5 регионов
  - Кораративный чемпионат Росатома Atomskills (Екатеринбург)
  - Digital Skills (Казань)
  - Чемпионаты СПО – 8 регионов (план)

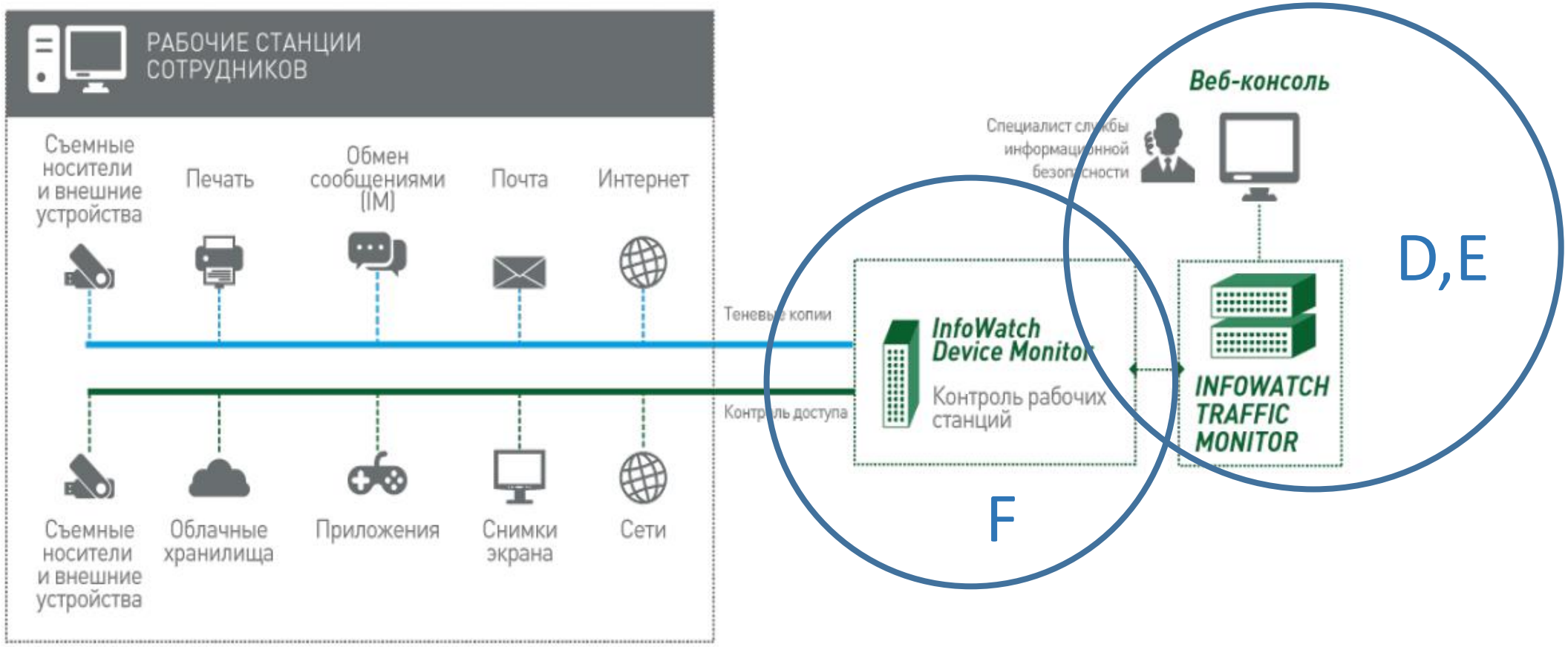
___ ___ 2018

Критерии компетенции «Корпоративная защита от внутренних угроз ИБ»

#	КРИТЕРИИ	ТИП
A	Организация работы и управление	Орг. навыки
B	Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	Linux, Windows администрирование DLP - установка
C	Исследование (аудит) организации с целью защиты от внутренних угроз	Нормативная база, аудит безопасности
D	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	DLP – применение (IW TM)
E	Поиск и предотвращение инцидентов. Технологии анализа сетевого трафика в системе корпоративной защиты информации от внутренних угроз	DLP – применение (IW TM - технологии)
F	Технологии агентского мониторинга	DLP – применение (IW DM)
G	Анализ выявленных инцидентов	DLP - отчёты

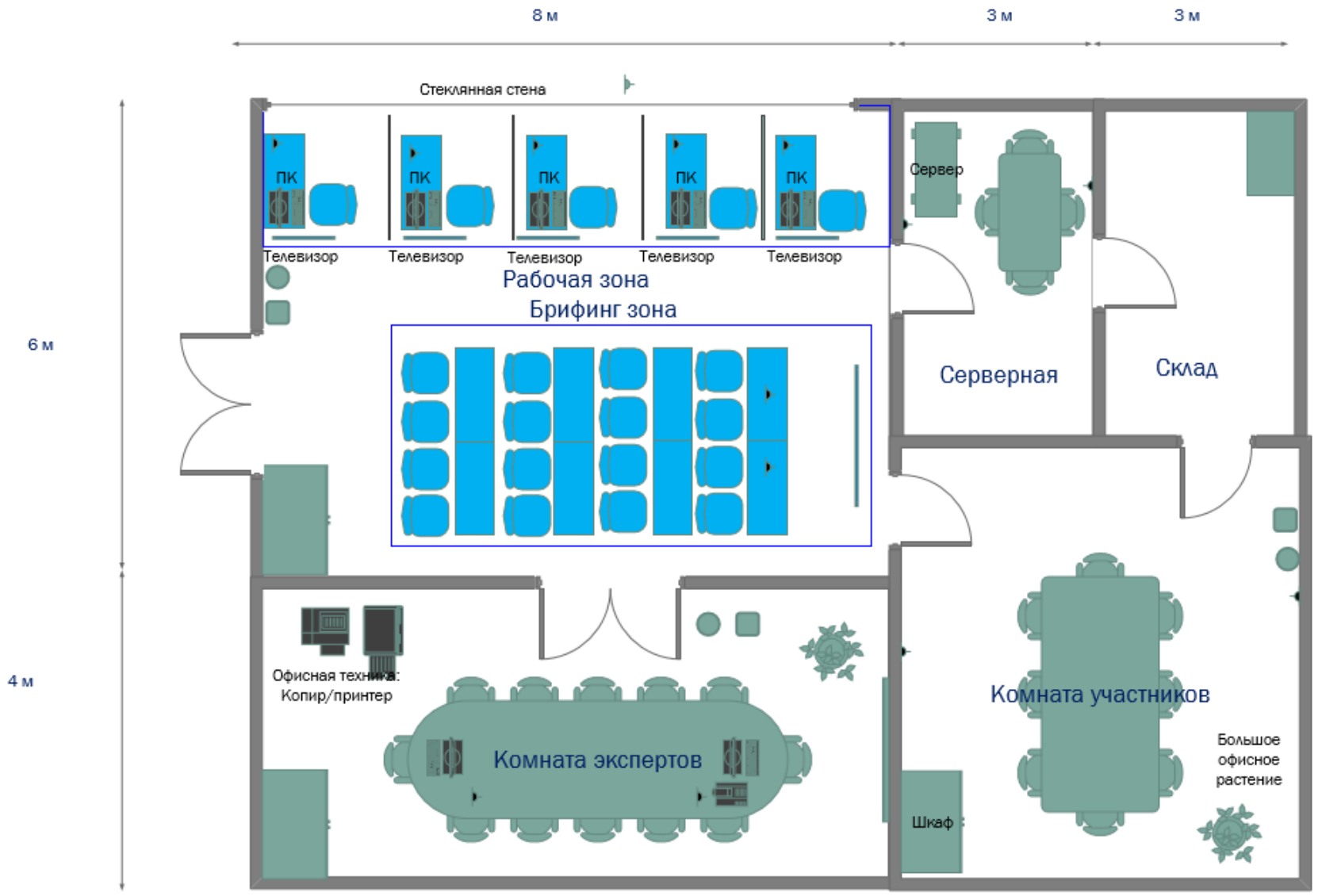
___ ___ 2018

Критерии компетенции «Корпоративная защита от внутренних угроз ИБ»



___ ___ 2018

Схема застройки



Инфраструктурный лист

Инфраструктура компетенции подразумевает развёртывание и использование полнофункциональной DLP-системы на заранее развёрнутой сетевой инфраструктуре.

- На каждого участника:
  - 1 ПК (для работы с DLP-системой)
    - CPU не ниже Intel Core i5 (с поддержкой виртуализации), RAM 16Gb, HDD 500Гб SATA.
    - ПО: VMWare Workstation или Oracle VB
    - Windows 10
  - 1 ноутбук (опционально, для имитации злоумышленника)
    - CPU не ниже Intel Core Duo, RAM 4 Gb, HDD 100 Гбайт
    - **Windows 10**
  - ПО: IWTM (виртуальная машина формата kickstart), IWDM Server(дистибутив), СУБД Postgres\СУБД Oracle (дистрибутив), файлы лицензий
- На всех участников:
  - Сетевая инфраструктура, каждый участник в отдельном VLAN
  - Домен Windows, 1 доменный сервер
- Специализированное ПО для проведения соревнований (предоставляется индустриальным партнёром компетенции): Генератор вредоносного траффика

___ ___ 2018

Модуль 3 и 4: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз. Поиск и предотвращение инцидентов. Технологии анализа сетевого трафика

- Создайте в системе InfoWatch Traffic Monitor политики безопасности согласно нижеперечисленным заданиям.
- Политики должны автоматически блокировать трафик или предупреждать о нарушении в соответствии с заданием.
- Некоторые политики должны быть созданы с нуля, некоторые могут быть сделаны путём модификации существующих в системе.
- Для некоторых политик необходима работа с разными разделами консоли управления TM: категориями и терминами, технологиями, объектами защиты и т.п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.
- При выявлении уязвимости, DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, участник должен самостоятельно задать уровень угрозы при разработке политики).
- Списки сотрудников, занимаемые позиции и отделы сотрудников (HR, Accounting и др.) представлены в разделе «Персоны» Infowatch Traffic Monitor по результатам LDAP-синхронизации с AD-сервером компании
- После создания всех политик, будет запущен автоматический «генератор трафика», который передаст на InfoWatch Traffic Monitor поток данных, содержащих как утечки, так и легальную информацию.
- При правильной настройке, политики InfoWatch Traffic Monitor должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний, т.к. легальные события не должны маркироваться как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.
- Необходимо называть политики/объекты/категории и прочие объекты в соответствии с заданием, например «***Политика Задание 2***». Без верно названных объектов проверка вашего задания может стать невозможной. **Стоит учесть, что совместно с созданными могут срабатывать стандартные политики, поэтому их стоит удалить или модифицировать**.

- В комплексных заданиях необходимо пользоваться объектами защиты.
- **Для некоторых заданий необходимы дополнительные файлы. Их можно найти в сетевой папке \\DL-DC-01\shared**
- Задания можно выполнять в любом порядке.
- Проверьте синхронизацию времени на всех системах, т.к. расхождение во времени между системами может повлиять на актуальность событий.
- Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.
- Все скриншоты необходимо сохранить на рабочем столе в папке «**Модуль 3**».
- Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: **CP-1.jpg**

1. где CP – сокращение от англ. *creating a policy*,
2. 1 – номер задания

Пример 2 для сохранения скриншота работающей политики: **PW-1.jpg**

1. где PW – сокращение от англ. *policy work*,
2. 1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики: **PW-1-2.jpg**

1. где PW – сокращение от англ. *policy work*,
2. 1 – номер задания;
3. 2 – номер скриншота для задания 1.

Модуль 3 и 4: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз. Поиск и предотвращение инцидентов. Технологии анализа сетевого трафика

Задание 1

Необходимо создать проверочную политику в InfoWatch Traffic Monitor на правило передачи текстовых данных за пределы компании (на адрес вне домена), содержащих аббревиатуры «Росатом-вооружение» и/или «ОМП», разрешить передачу, но установить средний уровень угрозы.

Аспекты	Направление	Файлы/комментарии
D1-1	Financial->External 4 передачи	4 срабатывания
E1-1 или E1-2	IT->IT 2 передачи	2 ложных

Задание 2

Необходимо создать новую категорию веб-ресурсов и добавить в нее следующие сайты: kb.infowatch.com, worldskills.org, vmware.com, demo.lab. Подтвердите выполнение задания скриншотами.

Аспекты	Направление	Файлы/комментарии
D1-2	Проверяется факт наличия категории	

Задание 4

Необходимо запретить передачу документов с грифом (информационной меткой) «ООО Demo Lab. Конфиденциально» или «ООО Demo Lab. Строго конфиденциально» сотрудникам за пределы компании. Исключение -- члены Совета директоров компании, имеющие право доступа к данной информации за пределами организации.

Обратите внимание, что при вводе информационной метки с клавиатуры сотрудники могут ошибаться и вводить между словами более 1 пробела или табуляции.

Уровень угрозы высокий, блокировать.

Аспекты	Направление	Файлы/комментарии
D1-3	IT->External	3 срабатывания
E1-5	External->IT	4 ложных
E1-7	IT->Financial	

___ ___ 2018

___ ___ 2018

Глава 4. Содержание профессиональных модулей основной профессиональной образовательной программы и методика преподавания профессиональных модулей с учетом стандарта Ворлдскиллс

Демонстрационный экзамен по стандартам WorldSkills

Демонстрационный экзамен – форма оценки соответствия уровня знаний, умений, навыков студентов и выпускников, осваивающих программы подготовки квалифицированных рабочих, служащих, специалистов среднего звена, позволяющих вести профессиональную деятельность в определенной сфере и (или) выполнять работу по конкретным профессии или специальности в соответствии со стандартами Ворлдсиллз Россияю

НОРМАТИВНАЯ РАМКА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ПО ОБРАЗОВАТЕЛЬНЫМ ПРОГРАММАМ СПО

Текущий этап и перспективы

- Перечень поручений по реализации Послания Президента Российской Федерации Федеральному Собранию от 4 декабря 2014 года № Пр-2821
- Распоряжение Правительства РФ от 3 марта 2015 года №349-р «Комплекс мер, направленных на совершенствование системы среднего профессионального образования»
- Федеральные государственные образовательные стандарты среднего профессионального образования по ТОП - 50 востребованных и перспективных профессий и специальностей на рынке труда
- Поручение Президента Российской Федерации от 23 декабря 2016 года № Пр-2852 по итогам встречи с членами национальной сборной России по профессиональному мастерству 9 декабря 2016 года

Демонстрационный экзамен

ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА ПО МЕТОДИКЕ ВОРДСКИЛС РОССИЯ

современное технологическое оборудование, позволяющее выполнить задание, приближенное к производственному, в количестве, достаточном для всей группы обучающихся, в сроки, отводимые на экзаменационные процедуры	**Специальные площадки**
контрольно-измерительные материалы, позволяющие объективно оценить достижения обучающихся	**Специальные инструменты оценки**
достаточное количество экспертов, способных оценить качество выполняемых работ	**Специально подготовленные кадры**

___ ___ 2018

Рекомендуемая учебно-методическая литература

- Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.
- Партыка Т.Л., Попов И.И. Информационная безопасность, учебное пособие. 5-е изд., перераб. и доп. - М.: ФОРУМ, 2012. - 432 с.
- Методические указания для выполнения лабораторных работ по курсу «Корпоративная защита от внутренних угроз информационной безопасности»;
- Техническое описание по компетенции «Корпоративная защита от внутренних угроз информационной безопасности», 2018, электронный документ
- Конкурсное задание по компетенции «Корпоративная защита от внутренних угроз информационной безопасности», 2018, электронный документ
- Инфраструктурный лист по компетенции «Корпоративная защита от внутренних угроз информационной безопасности», 2018, электронный документ
- План застройки по компетенции «Корпоративная защита от внутренних угроз информационной безопасности», 2018, электронный документ
- Положение об организации и проведении демонстрационного экзамена по стандартам WorldSkills Союза «Молодые профессионалы», электронная публикация
- Положение об организации и проведении демонстрационного экзамена по стандартам WorldSkills Союза «Молодые профессионалы», электронная публикация
- Приказ Департамента образования г. Москвы от 27 октября 2016 г. N 1118 "Об утверждении Положения о проведении демонстрационного экзамена с учетом требований стандартов WorldSkills в рамках государственной итоговой аттестации по образовательным программам среднего профессионального образования"
- Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (в ред. от 12.03.2014 N 35-ФЗ).
- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (в ред. от 19.12.2016 N 442-ФЗ)
- Федеральный закон "О национальной платежной системе" от 27.06.2011 N 161-ФЗ (в ред. от 03.07.2016 N 290-ФЗ)
- Примеры критериев оценки по компетенции «Корпоративная защита от внутренних угроз информационной безопасности», 2018, электронный документ
- Положение об организации и проведении демонстрационного экзамена по стандартам WorldSkills Союза «Молодые профессионалы», электронная публикация
- Кодекс этики ДВИЖЕНИЯ WORLDSKILLS RUSSIA, электронный документ, 2017
- Методические указания Минобрнауки России (Министерства образования и науки РФ) от 05 апреля 2017 г. №ЛО-47/06вн, 24 апреля 2017, электронный документ
- ПОЛОЖЕНИЕ о проведении Национального Межвузовского чемпионата «Молодые профессионалы (Ворлдскиллс Россия)», 2017, электронный документ

___ ___ 2018

ГУАП Государственный университет аэрокосмического приборостроения

Компетенция WSR «Корпоративная защита от внутренних угроз информационной безопасности»

Сергеев Антон Валерьевич,
менеджер компетенции WSR
abc@guap.ru, +7 911 232 07 69

2018