

Новые реалии в обучении информационной безопасности

Анна Чефранова
НОЧУ ДПО ЦПК
«Учебный центр «ИнфоТеКС»



Техно infotecs
2022 Фест

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Проблемы в подготовке специалистов в области защиты информации

ПРОБЛЕМЫ

* дефицит квалифицированных кадров по ИБ в организациях;

* неопределенность оценки объемов потребности в специалистах ИБ;

* недостаточная укомплектованность материально-технической базы образовательных учреждений;

* недостаточная подготовка преподавательского состава работе на современном оборудовании.

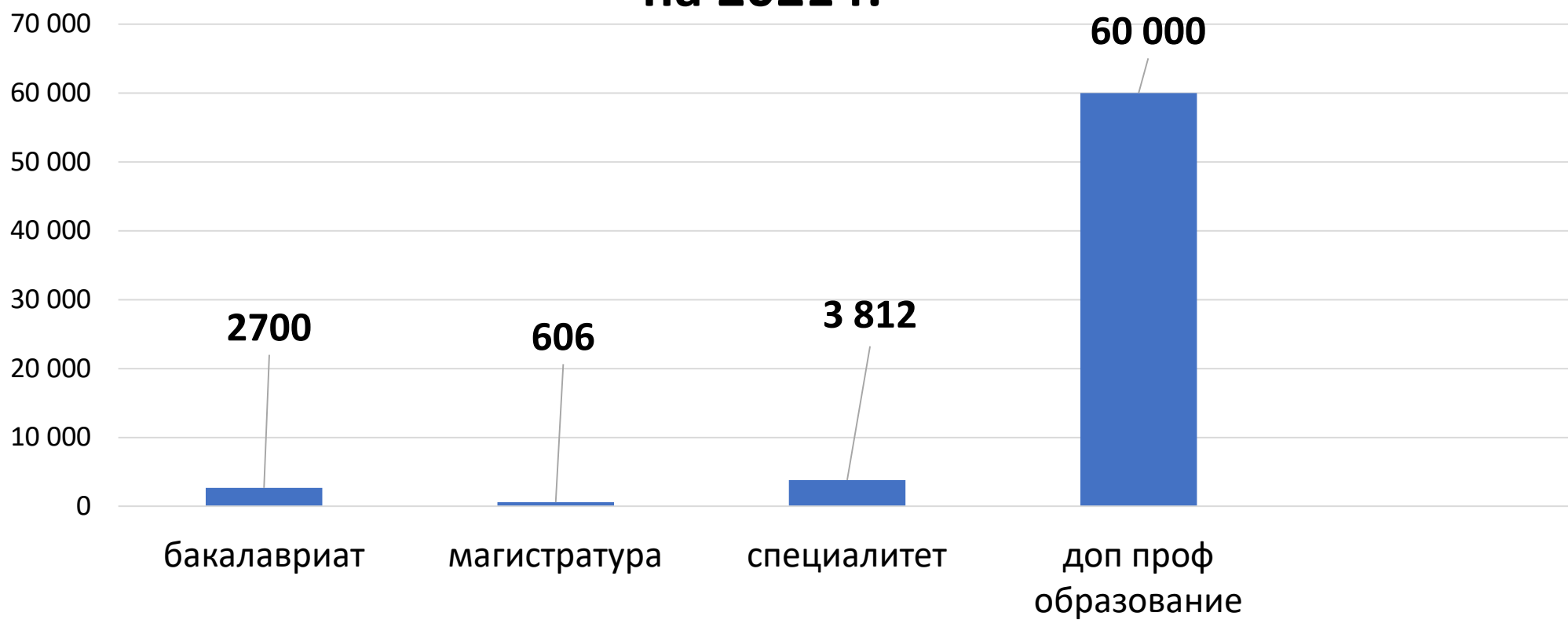
* Импортозамещение и безработица.

НОВОЕ в подготовке специалистов в области защиты информации

1. Новые образовательные стандарты в области ИБ.
2. Профессиональные компетенции и демозкзамен.
3. Требования – наличие лабораторий средств защиты информации.

Контрольные цифры (по данным ФУМО ИБ)

на 2021 г.



ТРЕБОВАНИЯ ФСТЭК

ПП «О внесении изменений в некоторые акты Правительства РФ по вопросам лицензирования отдельных видов деятельности»

Изменения, внесенные в Положение о лицензировании деятельности по технической защите конфиденциальной информации, утвержденное ПП РФ от 3 февраля 2012 г. № 79

**Лицензионные требования, предъявляемые к соискателю лицензии (юридическому лицу):
наличие в штате по основному месту работы в соответствии со штатным расписанием:**

1. Руководителя и (или) уполномоченного руководить работами по лицензионному виду деятельности лица, имеющего:

высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет

иное высшее образование и стаж работы по лицензируемому виду деятельности не менее 5 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения – не менее 360 аудиторных часов)

2. Инженерно-технических работников (не менее 2 человек), имеющих:

высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет

иное высшее образование и стаж работы по лицензируемому виду деятельности не менее 3 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения – не менее 360 аудиторных часов)

ТРЕБОВАНИЯ ФСБ

Приказ ФАПСИ от 13.06.2001 г. № 152

«Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

**Лицензионные требования,
предъявляемые к соискателю
лицензии (юридическому лицу):**

13. К выполнению обязанностей сотрудников органов криптографической защиты лицензиатами ФАПСИ допускаются лица, имеющие необходимый уровень квалификации для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ.

17. Обучение и повышение квалификации сотрудников органов криптографической защиты осуществляют организации, имеющие лицензию на ведение образовательной деятельности по соответствующим программам

21. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.

Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения.

ТРЕБОВАНИЯ МИНОБРА

Приказ № 1310 от 05.12.2013 г.

«Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»

Особенности разработки и реализации дополнительных профессиональных программ в области информационной безопасности




Пункт 18 Приказа определяет, что программы профессиональной переподготовки в области информационной безопасности утверждаются образовательной организацией по согласованию с ФСТЭК и/или ФСБ.

В данном контексте трактовать «и/или» можно так: все зависит от того, где вы дальше будете получать лицензию, на какой вид деятельности. Если ваша организация планирует получать лицензию в соответствии с Постановлением Правительства № 313, то, вам необходимо проходить профессиональную переподготовку по программе, согласованной с ФСБ. Если же вы планируете получать лицензию ФСТЭК, согласно Постановлению Правительства № 79, то для обучения подойдет программа, согласованная со ФСТЭК.

ТРЕБОВАНИЯ, изложенные в ПП № 1272 от 15.07.2022 г.

«Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»

Квалификационные требования к
ответственному лицу



II. Квалификационные требования к ответственному лицу

6. Ответственное лицо должно иметь высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Если ответственное лицо имеет высшее образование по другому направлению подготовки (специальности), он должен пройти обучение по программе профессиональной переподготовки по направлению "Информационная безопасность".

7. Для ответственного лица требуются наличие следующих знаний, умений и профессиональных компетенций:

- а) основные (в том числе производственные, бизнес и управленческие) процессы органа (организации) и специфика обеспечения информационной безопасности органа (организации);
- б) влияние информационных технологий на деятельность органа (организации), в том числе: роль и место информационных технологий (в том числе степень интеграции информационных технологий) в процессах функционирования органа (организации); зависимость основных процессов функционирования органа (организации) от информационных технологий;
- в) информационно-телекоммуникационные технологии, в том числе: современные информационно-телекоммуникационные технологии, используемые в органе (организации) и т.д.

Требования Минобразования и Минтруда Гармонизация ФГОС, ДПО и профессиональных стандартов



Направления работы учебного центра «ИнфоТеКС»

- ✓ Курсы по общим вопросам ИБ;
- ✓ Курсы профессиональной переподготовки по информационной безопасности;
- ✓ Курсы повышения квалификации по технологии ViPNet;
- ✓ Программа сотрудничества с образовательными учреждениями;
- ✓ Программа авторизованных учебных центров ИнфоТеКС;
- ✓ Участие в перспективных проектах по информационной безопасности.

Курсы по информационной безопасности

Курсы, согласованные со ФСТЭК и ФСБ:

- ✓ Информационная безопасность (512 часов)- проф переподготовка
- ✓ Информационная безопасность (106 часов) – повышение квалификации
- ✓ Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов КИИ (216 часов)- повышение квал.

Курсы по общим вопросам ИБ:

- ✓ Корпоративная защита от внутренних угроз информационной безопасности с использованием современных VPN технологий;
- ✓ Защита персональных данных в информационных системах персональных данных;
- ✓ Обеспечение требований по защите информации в финансовых организациях на основе действующего законодательства;
- ✓ И др.

Программы повышения квалификации по технологии ViPNet

Повышение квалификации по технологии ViPNet

Курсы по
ViPNet
Network
Security

Курсы по
ViPNet PKI

Курсы по
ViPNet
Industrial
Security

Курсы по
ViPNet Mobile
Security

Программы повышения квалификации по технологии ViPNet



ViPNet Mobile Security

- Технология ViPNet для защиты рабочих мест мобильных пользователей
- Пользователь ViPNet Connect



ViPNet Network Security

- Администрирование системы защиты информации ViPNet
- Программно-аппаратные комплексы ViPNet
- Пользователь системы защиты информации ViPNet
- Средства защиты информации ViPNet
- Программно-аппаратный комплекс ViPNet IDS +ViPNet TIAS
- Программно-аппаратный комплекс ViPNet xFirewall
- И др.



ViPNet PKI

- Удостоверяющий центр ViPNet
- Оператор Центра регистрации
- Пользователь ViPNet CSP
- ViPNet PKI Клиент
- И др.



ViPNet Industrial Security

- Защита промышленных систем с помощью технологии ViPNet
- Информационная безопасность в АСУ ТП электроэнергетики

Полный список курсов можно посмотреть на сайте infotecs-edu.ru

Работаем над будущим



Совместный проект ОАО «ИнфоТекС»
и МГУ имени М.В. Ломоносова



Клиент и сервер КРК



Шифраторы 10G

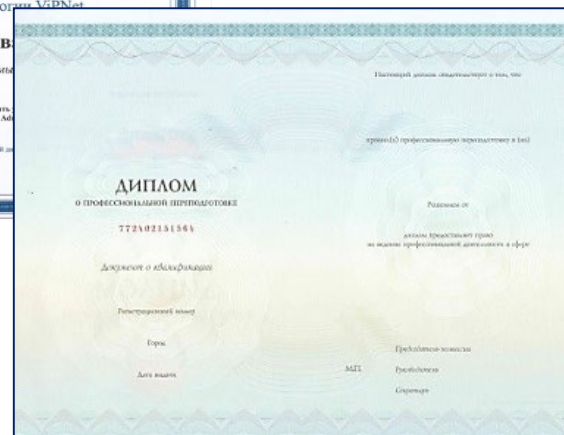
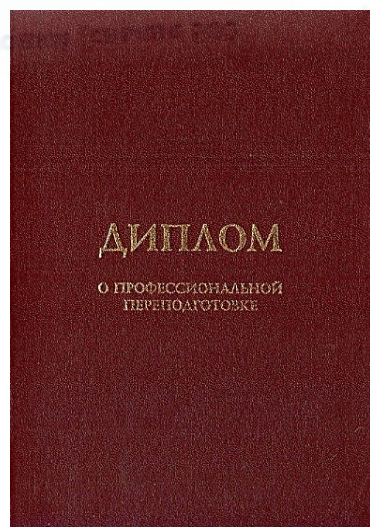
Распределенная
квантовая сеть



Выдаваемые документы

<https://infotecs-edu.ru/>

ОЧНОЕ ОБУЧЕНИЕ	ДИСТАНЦИОННОЕ ОБУЧЕНИЕ	ВЫЕЗДНОЕ ОБУЧЕНИЕ	ВЕБИНАРЫ	ТРЕНИНГИ
Программы переподготовки (свыше 500 часов)	Программы повышения квалификации (от 72 часов)	Программы повышения квалификации (от 16 часов)	Курсы по технологии ViPNet	



Очная/заочная формы обучения с использованием дистанционных технологий

1. Обучение по общим курсам ИБ (от 40 до 512 ак часов)

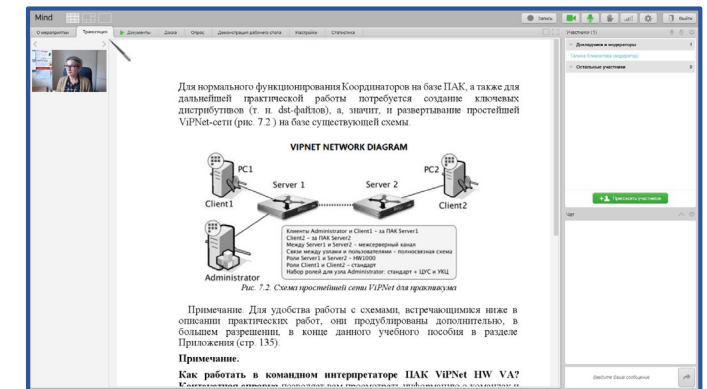
2. Курсы по технологии ViPNet (офлайн и онлайн)

3. Дистанционное тестирование

4. Очно-заочная формы учебных курсов

5. Вебинары

6. Дистанционная практика студентов



Программа авторизованных учебных центров «ИнфоТекС»

Авторизованные учебные центры «ИнфоТеКС» в РФ и СНГ



14 авторизованных
центров

Подготовка тренеров АУЦ

Курсы для тренеров АУЦ

* Новые программы обучения и тенденции развития рынка средств ЗИ;

* Особенности методики проведения курсов по технологии ViPNet;

* Актуальная информация о продуктовых линейках ViPNet;

* Направления сопровождения и помощи ГК «ИнфоТеКС» в организации обучения в АУЦ.



Выездные обучения

Санкт-Петербург, Архангельск, Калининград

Оренбург, Вологда, Курск, Магадан, Камчатка

Крым, Новороссийск, Ростов-на-Дону

Новосибирск, Томск, Барнаул, Екатеринбург

Казань, Самара, Волгоград,

И многие другие...

Всего вместе с АУЦ и выездными курсами –
обучаем 2000 человек в год



Приглашайте! Обучим в вашем городе!

chefr@infotecs.ru

Viktoria.Kashirina@infotecs.ru

Galina.Klimontova@infotecs.ru

Программа сотрудничества с образовательными учреждениями

Образовательные организации, участвующие в программе

Образовательные учреждения среднего
общего образования

Образовательные учреждения среднего
профессионального образования и профессионального
обучения

Образовательные организации высшего образования



Учебно-методический комплекс ViPNet (УМК ViPNet) это:

Учебно-методические комплексы ViPNet	
1.	Учебно-методический комплекс «Криптографическая защита информации»
2.	Учебно-методический комплекс «Криптографическая защита мобильных решений»
3.	Учебно-методический комплекс «Удостоверяющий центр»
4.	Учебно-методический комплекс «Межсетевые экраны»
5.	Учебно-методический комплекс «Криптографическая защита информации ViPNet туннель»
6.	Учебно-методический комплекс «Программно-аппаратная защита информации»
7.	Учебно-методический комплекс «Защита от несанкционированного доступа»
8.	Учебно-методический комплекс «Защита сетей»
9.	Учебно-методический комплекс «Корпоративная защита от внутренних угроз ИБ»

Учебно-методические пособия	
1.	Администрирование системы защиты информации ViPNet
2.	Программно-аппаратные комплексы ViPNet HW 4
3.	Удостоверяющий центр ViPNet
4.	Технология построения VPN ViPNet: курс лекций
5.	Программно-аппаратный комплекс ViPNet IDS
6.	Межсетевое экранирование
7.	Программно-аппаратные комплексы ViPNet: Курс лекций

Методические материалы	
1.	Плакаты УМК ViPNet

Желаете полноценную лабораторию?

Что входит в поставку:

- ✓ УМК
- ✓ Сценарии (учебные схемы)
- ✓ Обучение
- ✓ Обновления
- ✓ Консультирование

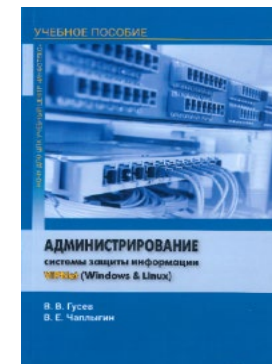
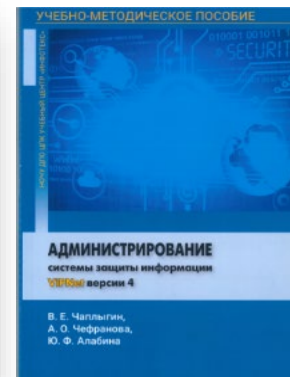
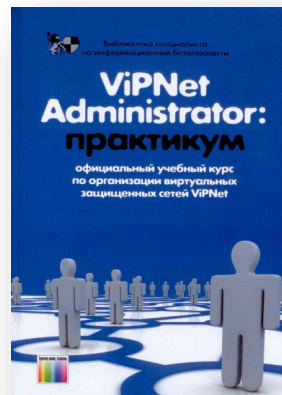
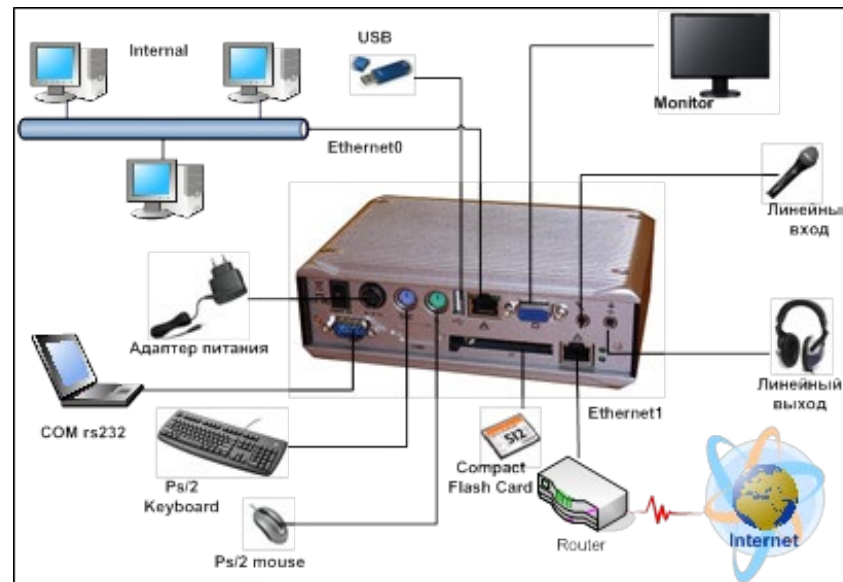
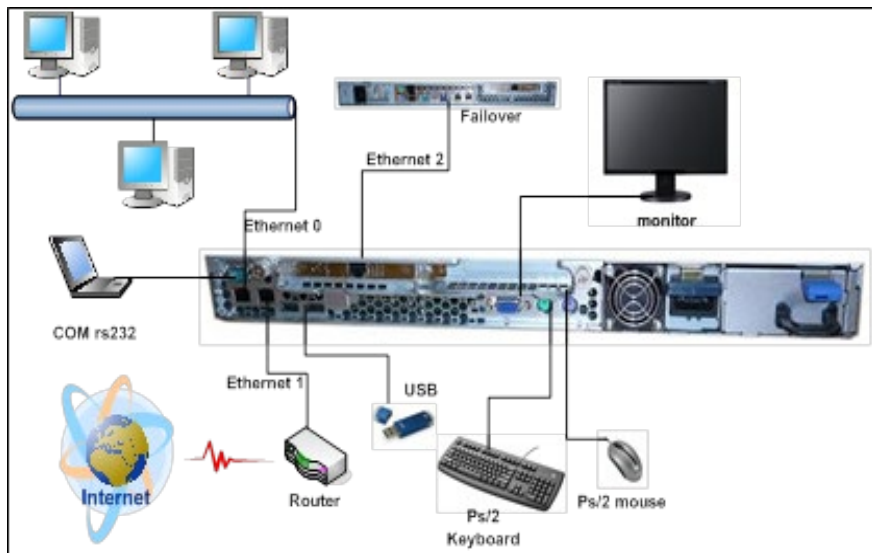
Для кого?

- ✓ ВУЗы, колледжи, школы
- ✓ Группы ВУЗов и колледжей + школы
- ✓ Крупные коммерческие компании (ГК) с большим количеством предприятий и площадок
- ✓ И др.

Пример готового класса



Стенды, оборудование, учебники



Мероприятия для образовательных учреждений

1. Семинары для вузов и колледжей в г. Москва и в регионах РФ;
2. Проведение мастер-классов;
3. Участие в Пленумах УМО по ИБ (ВПО и СПО);
4. Проведение интеллектуальных игр (хакатонов) по защите информации с помощью технологии ViPNet;
5. Организация и проведение Олимпиад по ИБ с заданиями по технологии ViPNet;
6. Участие в Демонстрационном экзамене;
7. Летние школы (для студентов последних курсов).



**Обновления:
будущее наступило вчера**



Проект по ранней профессиональной ориентации для учащихся «Билет в будущее»

Проект ИТ-классы

Задачи проекта:

1. Предпрофессиональная подготовка школьников к освоению профессий;
2. Обновление содержания образования по предмету «Информатика и ИКТ»;
3. Формирование разноуровневых компетенций.

Мероприятия:

1. С 2019 года ежегодно проводятся вебинары для руководителей, методистов и обучающихся школ;
2. Экскурсию в компанию «ИнфоТеКС» и учебный центр «ИнфоТеКС».
3. Стендовые доклады на форуме «Город образования».



Федеральный проект «Содействие занятости»

170
КОМПЕТЕНЦИЙ
в 7 профессиональных областях



Кто может обучаться?

Участниками Программы могут быть следующие категории граждан:

- граждане, ищущие работу и обратившиеся в органы службы занятости, включая безработных;
- лица в возрасте 50-ти лет и старше,
- лица предпенсионного возраста,
- женщины, находящиеся в отпуске по уходу за ребенком в возрасте до трех лет,
- женщины, не состоящие в трудовых отношениях и имеющие детей дошкольного возраста.

Проект «Цифровые профессии»

<https://цифровыепрофессии.рф/>



Центр компетенций по кадрам
для цифровой экономики

20.35
УНИВЕРСИТЕТ

Университет 2035

Условия проекта

180 000+

человек смогут обучиться
по программам дообразования
в сфере ИТ до 2024 года

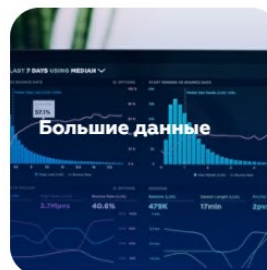
Участники

трудоспособные граждане РФ, возраст
16+, имеющие среднее
профессиональное и/или высшее
образование

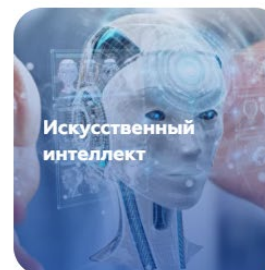
50%

стоимости обучения финансирует
государство

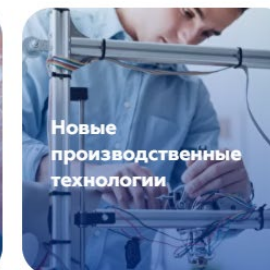
**Обучение на программах в области
программирования и ИТ-разработки
по востребованным в цифровой экономике
направлениям**



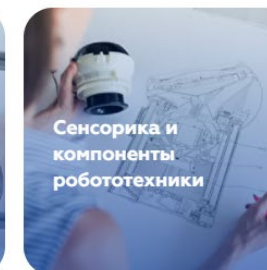
Больше данные



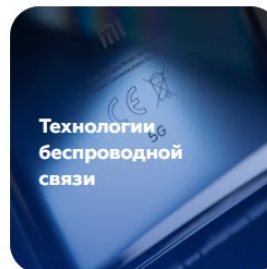
Искусственный
интеллект



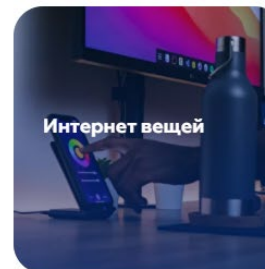
Новые
производственные
технологии



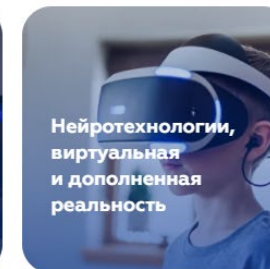
Сенсорика и
компоненты
робототехники



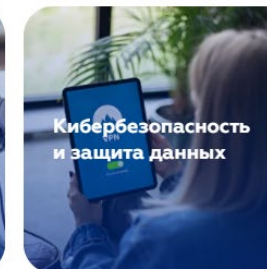
Технологии
беспроводной
связи



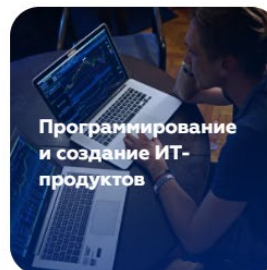
Интернет вещей



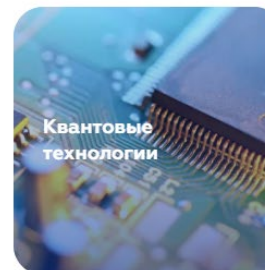
Нейротехнологии,
виртуальная
и дополненная
реальность



Кибербезопасность
и защита данных



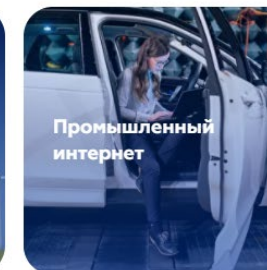
Программирование
и создание ИТ-
продуктов



Квантовые
технологии



Новые
и портативные
источники
энергии



Промышленный
интернет

Приглашаем к сотрудничеству:



Все свои предложения и вопросы вы можете отправлять:

education@infotecs.ru

Контактные телефоны:

+7 (495) 737-6192 (с 7:00 до 19:00 пн-пт)

+7 (495) 663-68-07

8-800-250-0-260 (по России бесплатно)

Адрес:

127083, г. Москва, ул. Мишина, д.56, стр.2, подъезд 2



ТЕХНО infotecs 2022 Фест

Спасибо за внимание!

Анна Чефанова
НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
chefr@infotecs.ru

Подписывайтесь на наши соцсети



https://vk.com/infotecs_news



https://t.me/infotecs_news