РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)
ИМЕНИ И.М.ГУБКИНА

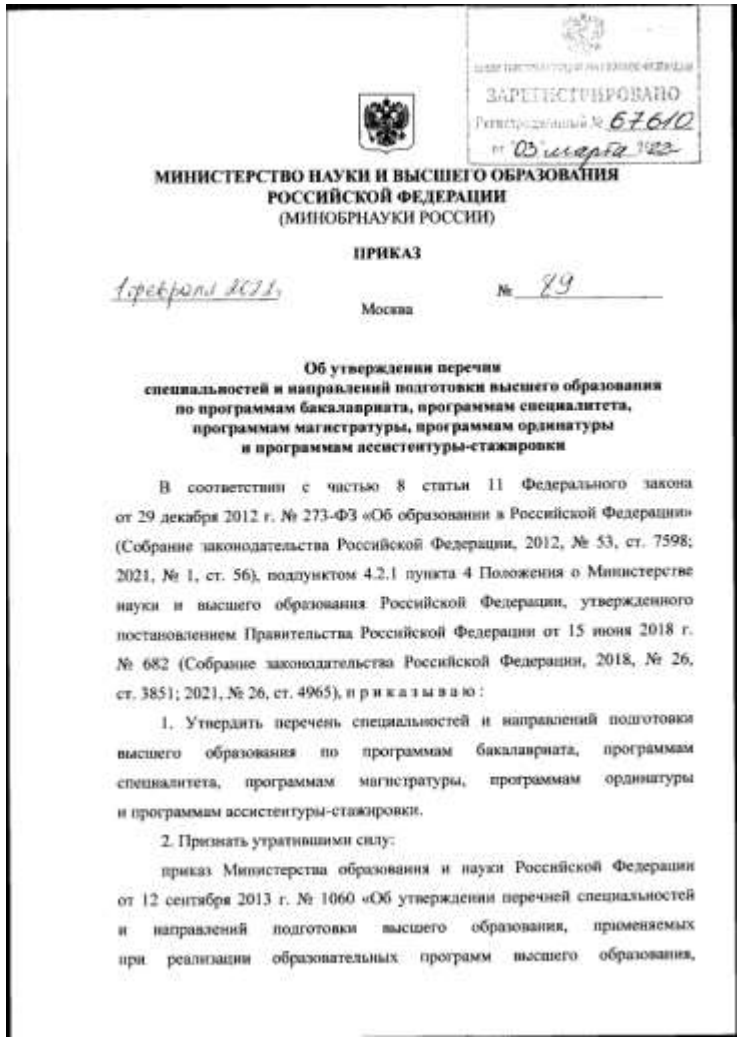
АКТУАЛЬНЫЕ ВОПРОСЫ ПОДГОТОВКИ КАДРОВ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ ТЭК

РЕШЕНИЯ ПОЛИТИЧЕСКОГО РУКОВОДСТВА

Поручение Президента Российской Федерации по результатам заседания Совета Безопасности Российской Федерации по вопросу:
«О совершенствовании подготовки кадров для обеспечения информационной безопасности Российской Федерации» от 6.12.2022. № Пр-2330.

Постановление Правительства Российской Федерации от 15.07.2022 № 1272 "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)"

ВЫХОД ИЗ БОЛОНСКОГО ПРОЦЕССА



ЗАРЕГИСТРИРОВАНО
Регистрационный № 67610
от 03 марта 2022

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ПРИКАЗ

1 февраля 2022 г. № 89

Москва

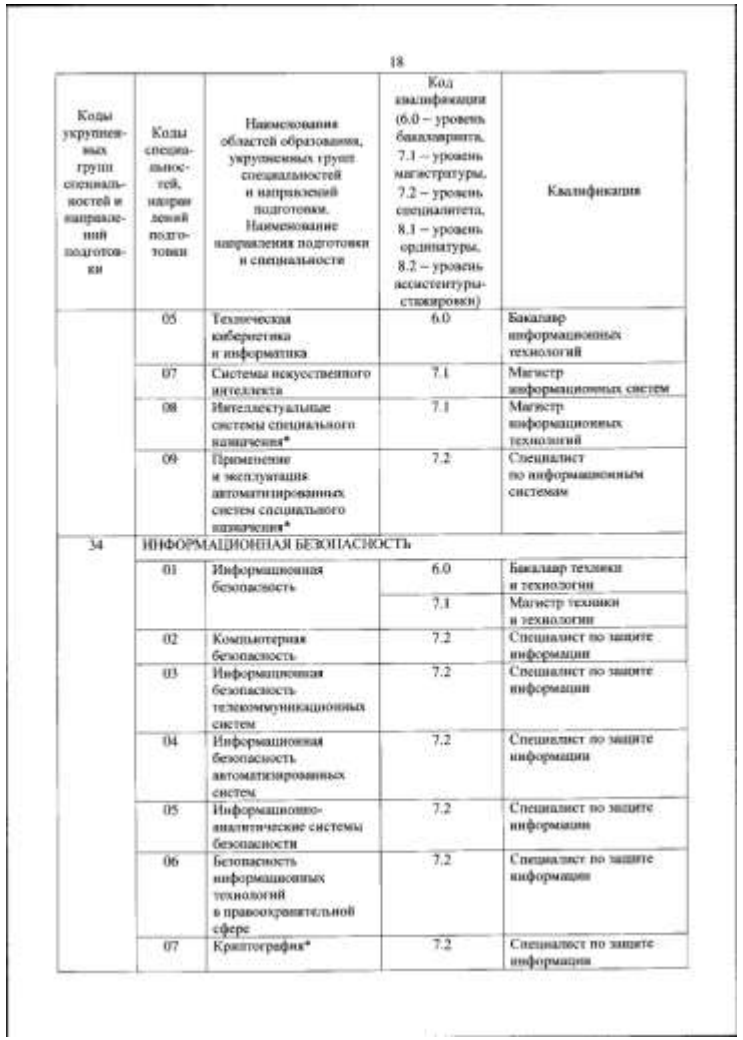
Об утверждении перечня специальностей и направлений подготовки высшего образования по программам бакалавриата, программам специалитета, программам магистратуры, программам ординатуры и программам ассистентуры-стажировки

В соответствии с частью 8 статьи 11 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, № 53, ст. 7598; 2021, № 1, ст. 56), подпунктом 4.2.1 пункта 4 Положения о Министерстве науки и высшего образования Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 15 июня 2018 г. № 682 (Собрание законодательства Российской Федерации, 2018, № 26, ст. 3851; 2021, № 26, ст. 4965), п р и к а з ы в а ю :

1. Утвердить перечень специальностей и направлений подготовки высшего образования по программам бакалавриата, программам специалитета, программам магистратуры, программам ординатуры и программам ассистентуры-стажировки.

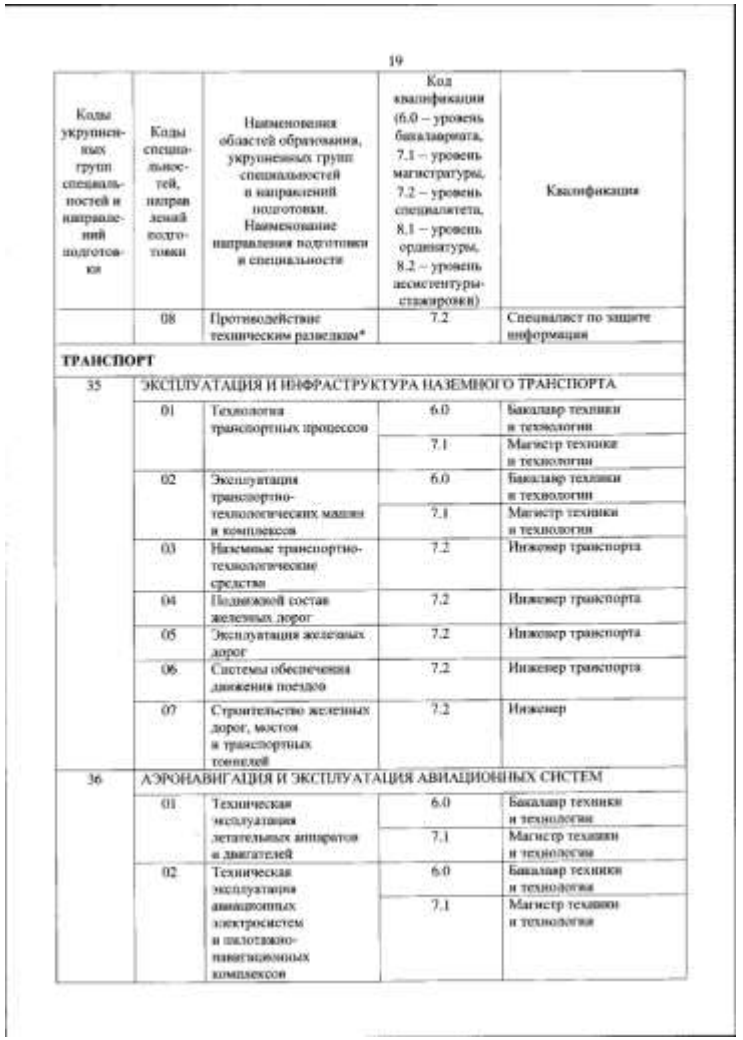
2. Признать утратившими силу:

приказ Министерства образования и науки Российской Федерации от 12 сентября 2013 г. № 1060 «Об утверждении перечней специальностей и направлений подготовки высшего образования, применяемых при реализации образовательных программ высшего образования,



18

Коды укрупненных групп специальностей и направлений подготовки	Коды специальностей, направлений подготовки	Наименования областей образования, укрупненных групп специальностей и направлений подготовки. Наименование направления подготовки и специальности	Код квалификации (6.0 – уровень бакалавриата, 7.1 – уровень магистратуры, 7.2 – уровень специалитета, 8.1 – уровень ординатуры, 8.2 – уровень ассистентуры-стажировки)	Квалификация
	05	Техническая кибернетика и информатика	6.0	Бакалавр информационных технологий
	07	Системы искусственного интеллекта	7.1	Магистр информационных систем
	08	Интеллектуальные системы специального назначения*	7.1	Магистр информационных технологий
	09	Применение и эксплуатация автоматизированных систем специального назначения*	7.2	Специалист по информационным системам
34	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ			
	01	Информационная безопасность	6.0	Бакалавр техники и технологии
			7.1	Магистр техники и технологии
	02	Компьютерная безопасность	7.2	Специалист по защите информации
	03	Информационная безопасность телекоммуникационных систем	7.2	Специалист по защите информации
	04	Информационная безопасность автоматизированных систем	7.2	Специалист по защите информации
	05	Информационно-аналитические системы безопасности	7.2	Специалист по защите информации
	06	Безопасность информационных технологий в правоохранительной сфере	7.2	Специалист по защите информации
	07	Криптография*	7.2	Специалист по защите информации



19

Коды укрупненных групп специальностей и направлений подготовки	Коды специальностей, направлений подготовки	Наименования областей образования, укрупненных групп специальностей и направлений подготовки. Наименование направления подготовки и специальности	Код квалификации (6.0 – уровень бакалавриата, 7.1 – уровень магистратуры, 7.2 – уровень специалитета, 8.1 – уровень ординатуры, 8.2 – уровень ассистентуры-стажировки)	Квалификация
	08	Противодействие техническим разведкам*	7.2	Специалист по защите информации
ТРАНСПОРТ				
35	ЭКСПЛУАТАЦИЯ И ИНФРАСТРУКТУРА НАЗЕМНОГО ТРАНСПОРТА			
	01	Технология транспортных процессов	6.0	Бакалавр техники и технологии
			7.1	Магистр техники и технологии
	02	Эксплуатация транспортно-технологических машин и комплексов	6.0	Бакалавр техники и технологии
			7.1	Магистр техники и технологии
	03	Наземные транспортно-технологические средства	7.2	Инженер транспорта
	04	Подвижной состав железных дорог	7.2	Инженер транспорта
	05	Эксплуатация железных дорог	7.2	Инженер транспорта
	06	Системы обеспечения движения поездов	7.2	Инженер транспорта
	07	Строительство железных дорог, мостов и транспортных тоннелей	7.2	Инженер
36	АЭРОНАВИГАЦИЯ И ЭКСПЛУАТАЦИЯ АВИАЦИОННЫХ СИСТЕМ			
	01	Техническая эксплуатация летательных аппаратов и двигателей	6.0	Бакалавр техники и технологии
			7.1	Магистр техники и технологии
	02	Техническая эксплуатация авиационных электросистем и пилотажно-навигационных комплексов	6.0	Бакалавр техники и технологии
			7.1	Магистр техники и технологии

Действие приказа приостановлено

ПРОФЕССИОНАЛЬНЫЕ СТАНДАРТЫ

В 2022 г. утверждены актуализированные шесть профессиональных стандартов в области ИБ

Планируемые к принятию в 2023 г.

- Специалист по криптографической защите информации
- Специалист по обеспечению безопасности значимых объектов КИИ ТЭК

Экспериментальные стандарты

- Специалист по защите персональных данных
- Специалист по противодействию кибермошенничеству

ОБРАЗОВАТЕЛЬНЫЕ СТАНДАРТЫ

Цель ФГОС – обеспечить единство образовательного пространства и государственные гарантии уровня и качества образования на основе единства требований к условиям реализации ООП и результатам их освоения

ФГОС 3+ и 3++

- Описание компетенций по каждой специальности и специализации

ФГОС 4

- Требования к результатам обучения по формированию каждой компетенции
- Компетенции:

- универсальные;
- базовые (отв. ФУМО);
- общепрофессиональные (отв. – ФУМО);
- профессиональные (отв. вуз).

ИЗМЕНЕНИЕ НОРМАТИВНОЙ БАЗЫ

Указ Президента Российской Федерации от 01.05.2022 г. № 250
«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

1. Руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (далее - органы (организации):

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

КОМПЕТЕНТНОСТЬ РУКОВОДИТЕЛЕЙ

Анонимный опрос центра компетенции Кибербезопасность «Энерджинет» НТИ, проведенный с целью с целью выявления наиболее острых проблем в области осведомленности и вовлеченности работников и руководства организаций в проблематику обеспечения информационной безопасности.

13) Проводится ли обучение ТОП менеджмента теоретическим вопросам ИБ?

Нет, обучение отсутствует даже в формальном виде.	46	50.0%
Да, проводится реальное обучение	24	26.1%
Да, формальные инструктажи (роспись в журнале)	22	23.9%

Ответов 92

13.1) Какие формы обучения теоретическим вопросам ИБ практикуются для ТОП менеджмента?

Общее со всеми работниками обучение основам ИБ и цифровой гигиены	14	35.9%
Специализированное обучение для ТОП менеджмента	12	30.8%
Общее со всеми работниками обучение и инструктажи по локальным нормативным актам (очные/заочные курсы и тестирование ...	10	25.6%
другое	3	7.7%

Ответов 39

14) Проводятся ли практические учения и тренировки для ТОП менеджмента по вопросам ИБ?

Нет	64	68.1%
О таком не известно (не знаю)	22	23.4%
Да	8	8.5%

Ответов 94

14.1) Какие формы учений и тренировок по вопросам ИБ практикуются для ТОП менеджмента?

Рассылка фишинговых писем	6	31.6%
«Штабные» учения	6	31.6%
Провокационные телефонные звонки	5	26.3%
Разбрасывание флешек в местах обитания ТОП менеджмента	2	10.5%
другое	0	0.0%

Ответов 19

ВОПРОС.
ТРЕБОВАНИЯ К КОМПЕТЕНЦИЯМ

ПК-1	Способен выделить основные (в том числе производственные, бизнес и управленческие) процессы предприятия ТЭК, определить роль и место информационных технологий при обеспечении их автоматизации, а также основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации
ПК-2	Способен определить основные угрозы безопасности информации для систем автоматизации предприятия ТЭК, предпосылки их возникновения и возможные пути их реализации, включая способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей
ПК-3	Способен планировать деятельность по обеспечению информационной безопасности на предприятии ТЭК, сформулировать цели, задачи, измеримые показатели уровня обеспечения информационной безопасности предприятия ТЭК, а также критерии их достижения
ПК-4	Способен обеспечить внедрение мер и средств обеспечения информационной безопасности критической информационной инфраструктуры предприятия ТЭК
ПК-5	Способен контролировать и анализировать состояние информационной безопасности на предприятии ТЭК
ПК-6	Способен организовать мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы предприятия ТЭК и реагированию на компьютерные инциденты

Компетенции, используемые для обучения по магистерской программе 10.04.01

ВОПРОС.
МЕТРИКИ ДЕЯТЕЛЬНОСТИ по ИБ

	Security Baseline: X			
Industry-Specific Controls	Industry-specific metric x%		Industry-specific narrative 1	
	Industry-specific metric x%		Industry-specific narrative 2	
	Metric		**How Measured**	**Progress Against Targets**
IT Controls	**Patching x % for Windows, Linux/Unix, Citrix**		% of systems in scope which meet agreed patching frequency	Trend of Patching
	IT Hardening	x%	% of compliant assets (x) within in-scope assets (x) which meet agreed targets	Trend of IT Hardening – Open deviations reduced by x from x – Forecasting x deviations will be cleared by x
	Cloud Hardening	x% x%	x public cloud 1 assets, of which x are fully compliant. x public cloud 2 assets, of which are fully compliant.	Trend of Cloud Hardening
	Anti-Malware Tools **Email Gateway Hygiene**	x x%	x assets covered across estate x active email domains across x business units	Trend of Anti-Malware Deployment
Security Tooling	**Endpoint Detection & Response (EDR) Coverage**	Tool 1 x% Tool 2 x%	Tool 1 software agents are deployed across x assets. (Compatibility for deployment of Tool 1 and Tool 2 agents is x% and y% respectively)	
	Web Application Firewall (WAF) Coverage	x%	% of websites behind a WAF with correct rules in blocking: x secured assets/x live assets	Trend of WAF Coverage – Coverage up x% year-over-year
Operational Metrics	**Phishing Results**	Non-click rate x%	Data based on year-to-date email phishing campaigns. x emails delivered across x locations. x users clicked on phishing tests from x test mails x%).	
	Security Incidents	x per month	Monthly incidents by severity	
	Vulnerabilities	x	Critical vulns open > x time period	Trend of Vulnerabilities – Number reducing with targeted actions

NOTES:
- *Key Risk Indicators (KRIs) shown in red under threshold, amber within range, green above threshold*
- *Target thresholds for KRIs shown in % are x % unless indicated*

Материал носит иллюстративный характер. Источник – блог А.Лукацкого

ЗАПРАШИВАЕМОЕ РЕШЕНИЕ

Вынести на комиссию Минэнерго России по обеспечению безопасности критической информационной инфраструктуры вопрос об организации на базе РГУ нефти и газа (НИУ) имени И.М.Губкина профессиональной переподготовки заместителей генеральных директоров предприятий ТЭК с учетом требований как Постановления Правительства Российской Федерации от 15.07.2022 № 1272 «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)», так и требований к профессиональным компетенциям, с учетом специфики предприятий ТЭК, а также метрикам / показателям деятельности по ИБ для предприятий ТЭК.