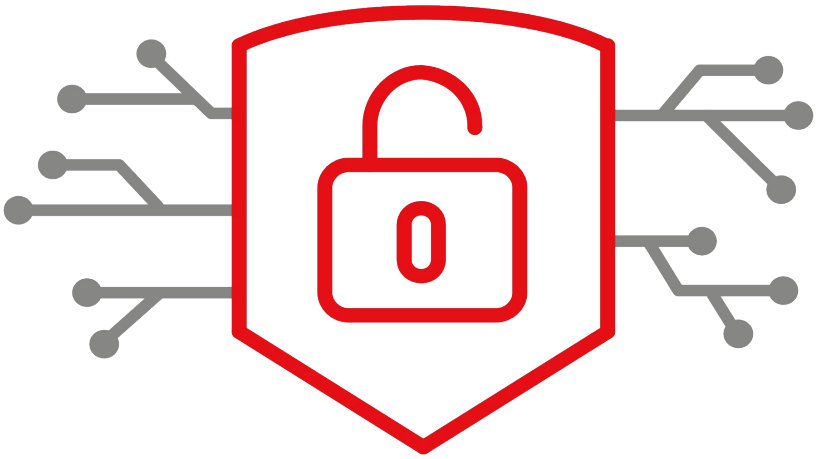


АНАЛИТИЧЕСКИЙ ОТЧЕТ

«Об образовании специалистов по информационной безопасности в Российской Федерации»

ПОДГОТОВЛЕН ЭКСПЕРТНОЙ ПОДГРУППОЙ ПО КИБЕРБЕЗОПАСНОСТИ

НТИ «ЭНЕРДЖИНЕТ»

2024

Содержание:

Аннотация

Настоящий отчет подготовлен экспертами центра компетенций «Кибербезопасность» Национальной технологической инициативы «Энерджинет» для выявления тенденций в области обеспечения подготовки специалистов по информационной безопасности в Российской Федерации, формирования комплексного взгляда, учитывающего мнения работодателей, профессионального сообщества и обучающихся.

В настоящее время в отношении образования в области информационной безопасности складываются противоречивые мнения, высказываемые как официально, в рамках различных форумах, так и неофициально, в том числе в частном порядке.

В отчёте приведены результаты анализа анонимного опроса, проводимого среди участников сообщества специалистов по информационной безопасности в Telegram в 2023 году.

Анализ изменений происходил путём сопоставления результатов опросов 2021 и 2023 года. Стоит отметить, что перечень вопросов, группы для проведения опросов, анализируемые параметры полностью идентичны.

Представляется, что именно анонимность опроса обеспечивает объективность его результатов, независимого от конъюнктуры среды или работы в конкретном предприятии или вузе.

Необходимо отметить, что исходя из названий и тематик сообществ возможно предположить, что большинство респондентов, принявших участие в опросе, в основном являются специалистами в области информационной безопасности и/или представляют компании, работающие в области информационной безопасности, являются потенциальными или фактическими работодателями для студентов, обучающихся по специальностям в области информационной безопасности.

Целью опроса является:

1. Определение тенденций в сфере подготовки специалистов в области информационной безопасности.
2. Выработка конструктивных подходов к решению выявленных проблем.

Отчёт предназначен для руководителей и специалистов, работающих в сфере информационной безопасности.

Структура системы образования специалистов

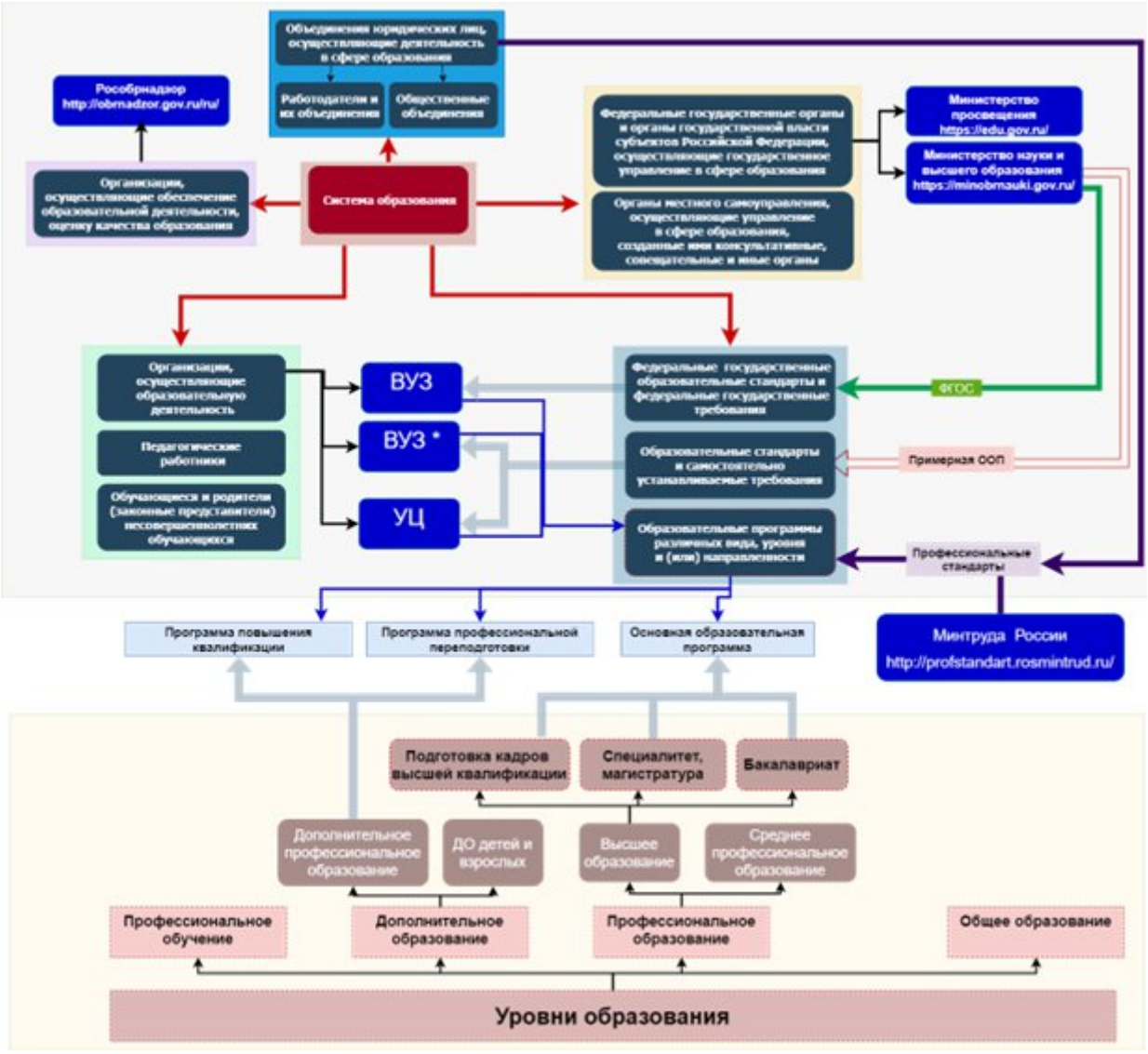


Схема 1. Обобщённая структура системы образования РФ.

24 мая 2022 г. министр науки и образования Валерий Фальков впервые заявил о планах ухода России от Болонской двухуровневой системы высшего образования — бакалавриата и магистратуры. На момент проведения опроса бакалавриат и магистратура в целом еще остаются как формы высшего образования в Российской Федерации. Вместе с тем, исходя из предложений ФУМО ИБ, в области высшего образования в сфере информационной безопасности основными формами будут специалитет и магистратура.

Профессиональные стандарты

По состоянию на август 2023 года в Российской Федерации действует 6 открытых профессиональных стандартов в области информационной безопасности и два стандарта, содержащих сведения ограниченного доступа.

В настоящее время ведётся разработка и публичное обсуждение 2 проектов новых проектов, а также обновление существующих профессиональных стандартов. Перечень стандартов и проектов представлен в Таблице 1

№	Код	Наименование	Год утверждения (обновления)
1	**Профессиональные стандарты**		
1.1	06.030	Специалист по защите информации в телекоммуникационных системах и сетях	2016 (2022)
1.2	06.031	Специалист по автоматизации информационно-аналитической деятельности	2022
1.3	06.032	Специалист по безопасности компьютерных систем и сетей	2016 (2022)
1.4	06.033	Специалист по защите информации в автоматизированных системах	2016 (2022)
1.5	06.034	Специалист по технической защите информации	2016 (2022)
1.6	06.053	Специалист по информационной безопасности в кредитно-финансовой сфере	2022
2	**Проекты профессиональных стандартов**		
2.1		Специалист по обеспечению безопасности значимых объектов критической информационной структуры	
2.2		Специалист по криптографической деятельности	
3	**Профессиональные стандарты, содержащий сведения, составляющие государственную тайну, или сведения конфиденциального характера**		
3.1	12.004	Специалист по обнаружению,	2016

		предупреждению и ликвидации последствий компьютерных атак	
3.2	12.005	Специалист по противодействию иностранным техническим разведкам	2016

Таб. 1. Перечень профессиональных стандартов в области информационной безопасности[1]

[1] С текстом стандартов и проектов можно ознакомиться на ресурсе Минтруда, https://profstandart.rosmintrud.ru, сайте Центрального банка Российской Федерации, https://cbr.ru и на сайте Межрегиональной общественной организации «Ассоциация защиты информации», https://azi.ru

Образовательные стандарты

На основании действующих профессиональных стандартов разработаны 13 федеральных государственных образовательных стандартов (ФГОС) охватывающих все уровни образования начиная со среднего специального и заканчивая высшей квалификацией. Перечень ФГОС представлен в Таблице 2.

№	Код	Наименование
	10.02.01	Организация и технология защиты информации
	10.02.02	Информационная безопасность телекоммуникационных систем
	10.02.03	Информационная безопасность автоматизированных систем
	10.02.04	Обеспечение информационной безопасности телекоммуникационных систем
	10.02.05	Обеспечение информационной безопасности автоматизированных систем
	10.03.01	Информационная безопасность
	10.04.01	Информационная безопасность
	10.05.01	Компьютерная безопасность
	10.05.02	Информационная безопасность телекоммуникационных систем
	10.05.03	Информационная безопасность автоматизированных систем
	10.05.04	Информационно-аналитические системы безопасности
	10.05.05	Безопасность информационных технологий в правоохранительной сфере
	10.06.01	Информационная безопасность

Таб. 2. Перечень ФГОС в области информационной безопасности[2]

Необходимо отметить, что в настоящее время идет активная разработка так называемого ФГОС 4.0 по укрупненной группе специальностей «Информационная безопасность», который учитывает как складывающиеся тенденции в высшем образовании в целом (в частности, отказ от Болонской системы), так и актуальный перечень образовательных специальностей и специализаций. Текущая обсуждаемая версия ФГОС 4.0 контролируется ФУМО ИБ и может быть получена по запросу в любом виде.

[2] С текстом ФГОС можно ознакомиться на ресурсе Национальной ассоциации развития образования и науки, https://fgos.ru/

Результаты исследования

Значительную долю опрошенных в 2023 году составили потребители ИБ и ИТ услуг, а также интеграторы (37% и 30% соответственно). Данные лица (работники организаций интеграторов, потребителей услуг) фактически выступают в двух ипостасях: как конечные заказчики результатов внедрения ИБ решений и как работодатели для специалистов, которые должны проектировать и внедрять решения ИБ. Вместе с тем, подавляющее большинство опрошенных отмечает недостаточность практических (82%) и(или) теоретических (57%) знаний выпускников. Таким образом, получается, что конечные потребители, скорее всего, через опыт своей работы не вполне удовлетворены качеством образования в сфере информационной безопасности.

Можно предполагать, что одним из ключевых моментов в обеспечении качества образования являются профессиональные и образовательные стандарты, точнее их взаимно-однозначная связка. Опрос показал, что в целом опрошенные знают о существовании образовательных стандартов и готовы участвовать в их разработке/совершенствование (57%).

Следующим моментом, на который следует обратить внимание, является то, что в образовательных стандартах ключевым является сочетание общепрофессиональных и профессиональных компетенций. Для практической работы важно сочетание профессиональных компетенций и знаний предметной области. Поэтому понимание и требования к специалистам информационной безопасности трансформируется от общего к частным. Вместе с тем, 51% опрошенных считает, что специализация по ИБ узкого профиля (например, аналитик уязвимостей, пентестер, аудитор и т.п.) не нужна. Согласно опросу, выпускники соответствуют требованиям работодателя (полностью или в основном) в 27% случаев. Значит, они должны либо самостоятельно, либо под руководством специалистов организации суметь адаптироваться под новые обстоятельства (под выполнение тех функций и задач, которые входят в их должностные обязанности и планы рыбот). Соответственно, здесь уже в большей степени играет роль не набор конкретных знаний и умений, а способность адаптироваться к изменившимся обстоятельствам.

Вовлеченность специалистов в систему образования

89,6 % опрошенных знают про существование образовательных стандартов (диаграмма 1).

При этом 52,1% опрошенных читали образовательные стандарты и 24,1% считают, что от образовательных стандартов что-то зависит (диаграмма 2.)

Данные сопоставимы с результатами опроса 2021 года. Тогда было 88,1 / 43,9 / 10,9 соответственно.

Стоит отметить, что процент опрошенных, считающих что от образовательные стандарты имеют влияния по прежнему мал, но в 2,5 раза выше чем был 2 года назад.

Диаграмма 1. Знание образовательных стандартов образовательных

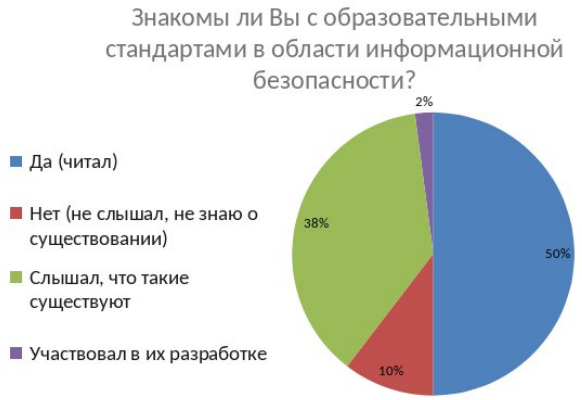


Диаграмма 2. Роль образовательных стандартов

Диаграмма 3. Необходимость в изменение образовательных стандартах

Диаграмма 4. Готовность участвовать в разработке образовательных стандартов

Система подготовки специалистов

Не изменилось мнение опрошенных относительно необходимости узкой специализации специалистов. 52% за узкую специализацию и 48% против неё в 2021 году и 51,1% и 48,9% в 2023 году соответственно.

Диаграмма 5. Необходимость узкой специализации

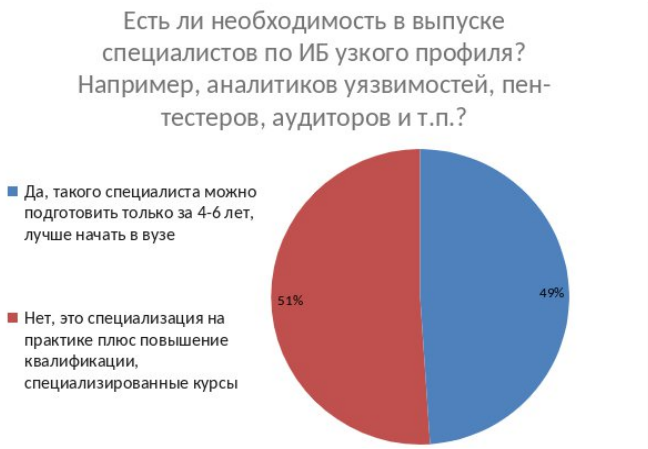


Диаграмма 6. Необходимость отраслевой специфики в образование

64% за последние 3 года принимали на работу выпускников, имеющих образование в области информационной безопасности.

22% были приняты на инженерную позицию

23% были приняты на позицию специалиста

19% были приняты на стажерскую позицию.

В опросе 2021 года, брали на работу выпускников 77% опрошенных.

Диаграмма 7. Необходимость бакалавров

Диаграмма 8. Соответствие подготовки выпускников требованиям заказчика

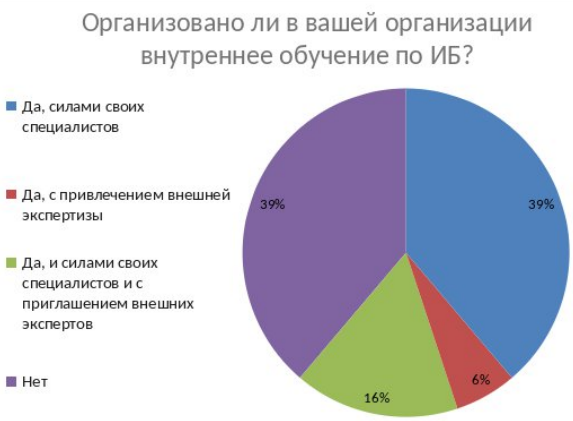
Диаграмма 9. Оценка подготовленности выпускников

Послевузовское образование

88,9% работодателей респондентов обеспечивают обучение работников и только у 38,8% опрошенных отсутствует внутреннее обучение по ИБ.

Диаграмма 10. Оплата обучения работодателем

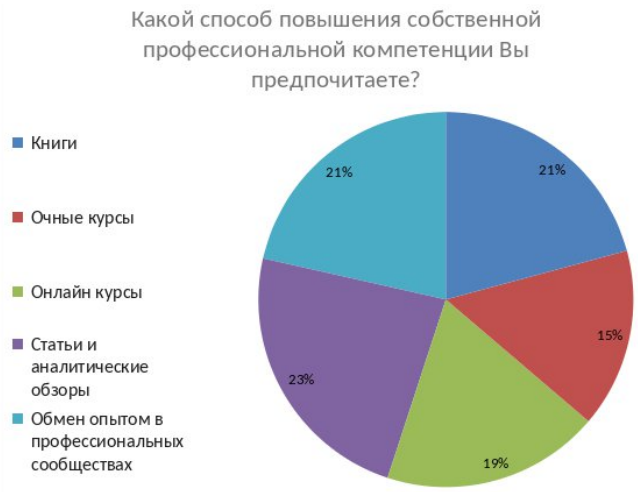
Диаграмма 11.. Внутреннее обучение по ИБ



73,3% специалистов готовы оплачивать повышение своей квалификации. При этом, лишь треть опрошенных предпочитаю повышение квалификации на курсах.

Диаграмма 12. Самостоятельная оплата обучения

Диаграмма 13. Приоритетный способ повышения квалификации



Данные показатели 2021 и 2023 годов можно считать идентичными.

В 2021 году 82,4% обучали, 30,5% отсутствует внутреннее обучение и 72,6% готовы оплачивать образование сами.

При этом в 2023 году равный интерес среди респондентов в обучении вызвали:

- отдельные технические мер защиты (31,8%),
- обучение законодательству (27,1%),
- обучению реализации организационных мер (23,3%).

Хотя в 2021 году основной ориентир был на технические меры защиты (49,3%) и законодательство (26,7%).

Диаграмма 14. Приоритетные направления обучения

Диаграмма 15. Приоритетные типы курсов повышения квалификации

Вместе с тем, изменился и спрос на методологическую базу:

2021 г. - 22,5% против 22,1% в вопросах выбора российской или иностранной методологической базы

2023 г. - 39,2% против 11.8% соответственно.

Диаграмма 16. Комфортность изучения зарубежных документов

Диаграмма 17. Разнообразие курсов на русском языке

Диаграмма 18. Качество курсов на русском языке

Анализ результатов исследования

Данное исследование проводилось для анализа изменений ситуации в образовательной сфере. Для этого участникам опроса были заданы вопросы, используемые для аналитического отчёта в 2021году[3], который также проводил центр компетенций «Кибербезопасность» НТИ Энерджинет.

Общее состояние дел и показатели опросов идентичны между собой. Поэтому в данном отчёте приведено значительно меньше справочной информации, а также отсутствует блок анализа самих показателей. Считаем аналитику прошлого отчёта в целом актуальной.

Вместе с тем, стоит обратить внимание на изменения показателей между отчёта и сделать соответствующие выводы.

Первое, что стоит отметить - увеличенное внимание участников рынка к образованию: Почти в 1,5 раза выросло число людей, готовых участвовать в разработке и совершенствовании стандартов (с 40% до 57%)

Во вторых, почти в 2 раза возросла удовлетворённость выпускниками ВУЗов (с 15% до 27%).

В третьих, если ранее основной интерес вызывали курсы по техническим мерам защиты, то сейчас спрос на технические, организационные меры и требования законодательство распределены практически поровну (31,8%, 23,3% и 27,1% соответственно).

А также изменился приоритет в методологической базе. Он стал ориентирован на российские базы знаний и практик.

Возможно требуется формирование общественного мнения и прозрачной стратегии государства в вопросе специализации (например, аналитик уязвимостей, пентестер, аудитор и т.п.). Опрошенные стабильно почти в равных долях считают что узкоспециализированные нужны и не нужны (51,1% соответственно).

При это остаётся высоким число тех, кто считает что необходима отраслевая специфика в ИБ (75% -2021 г.; 89% - 2023 г.)

[3] С результатами прошлого отчёта можно ознакомиться по ссылке: https://github.com/SecureEnergynet/Research

Выводы

Успешное развитие подготовки специалистов по информационной безопасности в Российской Федерации требует осознанного участия всех заинтересованных сторон, включая представителей государственных и частных организаций в интересах которых в конечном итоге и будут трудиться специалисты.

По результатам опроса обращает на себя внимание значительная смена ориентации опрашиваемых с зарубежной методологической базы на российскую. Это отражает активные изменения в связи с импортозамещением. Растёт спрос на имеющиеся российские методологии, технические решения и практики их применения.

Растёт удовлетворённость выпускниками ВУЗов. При этом сами показатели остаются достаточно низкими.

Возможно, в полтора раза увеличенное внимание участников сферы ИБ (регуляторы, предприятия, интеграторы, производители средств защиты информации) к образованию даёт положительные эффекты.

Компании в два раза активнее интересуются образованием в части организационных мер. Это может говорить о том, что системы ИБ более активно используются в деятельности компаний, и возникает потребность в знаниях по организации и оптимизации данных процессов.

Вместе с тем, потребность в создание системы подготовки и развития кадров, удовлетворяющий участников рынка, остаётся открытой.

Обозначенные в прошлом отчёте пути решения остаются актуальными:

- Создание и предоставление студентам бесплатного доступа к национальным полигонам, позволяющим студентам отрабатывать практические задачи по эксплуатации всех имеющихся на рынке средств защиты.
- Вовлечение всех участников рынка для прохождения студентами производственной и преддипломной практики на реальных предприятиях, а не выполнение синтетических задач на профильных кафедрах.

Также стоит отметить, что до недавнего времени обеспечение специалистами по информационной безопасности фактически приравнивалось к их подготовке в рамках высшего образования по направлению информационная безопасность. Требовались исполнители, способные выполнять зачастую работу по бумажной безопасности, не связанной с деятельностью компании.

В последнее время акцент начал смещаться в сторону применения ИБ как действующего инструмента устойчивости работы сервисов и бизнеса, а следовательно формирование относительно крупных отделов ИБ. Для этого требуется кадровое обеспечение, которое подразумевает подготовку специалистов со средним специальным образованием, профессиональную переподготовку, повышение квалификации и другие формы образования.

Фактически рынок труда специалистов по информационной безопасности за последние 2 года претерпел сильные изменения, которые связаны как с импортозамещением, так и с появлением целого ряда новых специализаций (например, специалист по безопасной разработке программного обеспечения).

Как следствие, необходимо создание и описание траекторий карьерного пути развития в сфере ИБ. Данная карта представляет из себя интеграцию сводной информации по фактически открытым вакансиям на рынке труда, а также имеющимся образовательным и профессиональным стандартам. Карта сможет наглядно показывать имеющиеся различия, а также помогать проложить свой путь обучения и развития для каждого желающего.

Также предлагается обратить внимание на мотивацию студентов и специалистов из смежных отраслей развиваться в сфере информационной безопасности.

Решением может стать формирование целостной концепции кадрового обеспечения сферы информационной безопасности, которая учитывала бы особенности среднего специального образования, высшей школы, различных образовательных центров, учебных подразделений (академий) вендоров и т.д.

В рамках центра компетенций «Кибербезопасность» НТИ Энерджинет ведутся работы по предлагаемым путям улучшения ситуации. Приглашаем к взаимодействию.

Отчет подготовлен рабочей группой в составе: А.В. Петухов, Д.И. Правиков, М.Б. Смирнов, Гуревич А. Ю., Никандров М. В.

Приложение 1

Должности и трудовые функции, предусмотренные профессиональными стандартами в сфере информационной безопасности

	Требования к образованию и обучению	**Возможные наименования должностей, профессий**	**Обобщенные трудовые функции**
	Специалист по защите информации в телекоммуникационных системах и сетях		
	Среднее профессиональное образование	Техник по защите информации I категории Техник по защите информации II категории Техник по защите информации Старший техник по обслуживанию телекоммуникационного оборудования	Выполнение комплекса мер по обеспечению функционирования СССЭ и (за исключением сетей связи специального назначения) и средств их защиты от НСД
	Бакалавриат	Инженер по защите информации Инженер по телекоммуникациям Администратор телекоммуникационного оборудования	Обеспечение защиты от НСД сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации
	Бакалавриат и повышение квалификации	Инженер специальной связи Инженер по защите информации	Обеспечение функционирования средств связи сетей связи специального назначения
	Специалитет или магистратура	Инженер-программист I категории Инженер-программист II категории	Разработка средств защиты СССЭ (за исключением сетей связи специального назначения) от НСД

		Инженер-программист III категории Инженер-программист Инженер-проектировщик I категории Инженер-проектировщик II категории Инженер-проектировщик III категории Инженер-проектировщик Руководитель проектов Специалист по защите информации I категории Специалист по защите информации II категории Специалист по защите информации	
	Специалитет или магистратура	Старший инженер Старший инженер-разработчик Старший инженер специальной связи Консультант по специальным телекоммуникациям	Обеспечение защиты средств связи сетей связи специального назначения от НСД
	Специалитет или магистратура	Начальник (руководитель) отдела (отделения) систем защиты информации Ведущий инженер-разработчик	Управление развитием средств и систем защиты СССЭ от НСД
	Специалитет или магистратура	Начальник (руководитель) научно-исследовательского отдела (лаборатории) Ведущий (главный) специалист по защите информации	Экспертиза проектных решений в сфере защиты СССЭ от НСД

		Научный консультант по защите информации	
	Специалист по безопасности компьютерных систем и сетей		
	Среднее профессиональное образование	Техник по безопасности компьютерных систем и сетей Техник по защите информации I категории Техник по защите информации II категории Техник по защите информации	Обслуживание средств защиты информации в компьютерных системах и сетях
	Бакалавриат	Администратор безопасности компьютерных систем и сетей Администратор по обеспечению безопасности информации Инженер-программист по технической защите информации I категории Инженер-программист по технической защите информации II категории Инженер-программист по технической защите информации Инженер-программист I категории Инженер-программист II категории Инженер-программист III категории Инженер-программист	Администрирование средств защиты информации в компьютерных системах и сетях
	Специалитет или магистратура	Специалист по защите информации в компьютерных системах и сетях	Оценивание уровня безопасности компьютерных систем и сетей

		Эксперт по анализу защищенности компьютерных систем и сетей Ведущий (старший) специалист по защите информации Руководитель группы (специализированной в прочих отраслях) Руководитель группы (функциональной в прочих областях деятельности)	
	Специалитет или магистратура и повышение квалификации или аспирантура	Главный специалист по защите информации Руководитель отдела систем защиты информации Заместитель руководителя департамента (отдела) исследований и разработок Руководитель департамента (отдела) исследований и разработок	Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей
	Специалист по защите информации в автоматизированных системах		
	Среднее профессиональное образование	Техник по защите информации I категории Техник по защите информации II категории Техник по защите информации	Обслуживание систем защиты информации в автоматизированных системах
	Бакалавриат	Инженер по защите информации Специалист по защите информации I категории Специалист по защите информации II	Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации

		категории Специалист по защите информации Инженер-программист по технической защите информации I категории Инженер-программист по технической защите информации II категории Инженер-программист по технической защите информации Инженер-программист I категории Инженер-программист II категории Инженер-программист III категории Инженер-программист	
	Бакалавриат	Инженер по защите информации Специалист по защите информации I категории Специалист по защите информации II категории Специалист по защите информации Инженер-программист по технической защите информации I категории Инженер-программист по технической защите информации II категории Инженер-программист по технической защите информации	Внедрение систем защиты информации автоматизированных систем

		Инженер-программист I категории Инженер-программист II категории Инженер-программист III категории Инженер-программист	
	Специалитет или магистратура	Ведущий инженер-разработчик систем защиты информации Ведущий специалист по защите информации Руководитель проектов в области разработки систем защиты информации Руководитель отдела систем защиты информации	Разработка систем защиты информации автоматизированных систем
	Специалитет или магистратура и повышение квалификации или аспирантура	Главный специалист по защите информации Руководитель отдела систем защиты информации Заместитель руководителя департамента (отдела) исследований и разработок Руководитель департамента (отдела) исследований и разработок	Формирование требований к защите информации в автоматизированных системах
	Специалист по технической защите информации		
	Среднее профессиональное образование	Техник по технической защите информации I категории Техник по технической защите	Проведение работ по установке и техническому обслуживанию средств защиты информации

		информации II категории Техник по технической защите информации	
	Бакалавриат	Специалист по технической защите информации I категории Специалист по технической защите информации II категории Специалист по технической защите информации Инженер по технической защите информации	Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации Производство, сервисное обслуживание и ремонт средств защиты информации Проведение контроля защищенности информации
	Специалитет или магистратура	Специалист по технической защите информации I категории Специалист по технической защите информации II категории Специалист по технической защите информации Инженер по технической защите информации	Разработка средств защиты информации Проектирование объектов в защищенном исполнении
	Специалитет или магистратура и повышение	Специалист по технической защите информации I категории Специалист по технической защите информации II категории	Проведение аттестации объектов на соответствие требованиям по защите информации Проведение сертификационных испытаний средств

	квалификации	Специалист по технической защите информации Инженер по технической защите информации	защиты информации на соответствие требованиям по безопасности информации
	Специалитет или магистратура и повышение квалификации или аспирантура	Главный специалист по технической защите информации Руководитель структурного подразделения по технической защите информации	Организация и проведение работ по технической защите информации