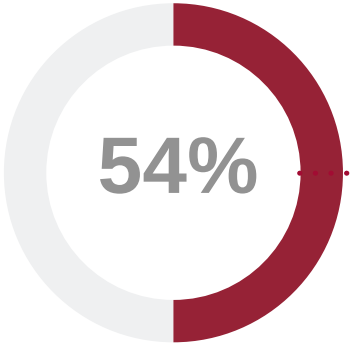
академия softline

Подготовка кадров для объектов КИИ: опыт и перспективы

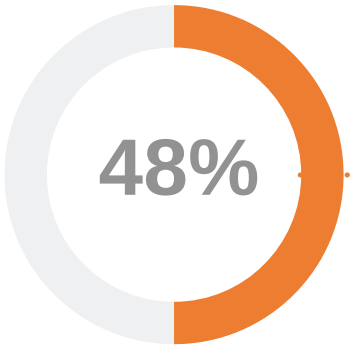
Игорь Семенихин
Кандидат военных наук, доцент,
Директор Центра исследования интернета вещей ФГБУ НИИР, ведущий эксперт Академии Softline

Через обучение - к успеху!
Знания работают на вас

Дефицит кадров в области Информационной безопасности



Российских компаний испытывают дефицит специалистов по информационной безопасности



Субъектов КИИ отмечают недостаток квалифицированных ИБ-специалистов

На одну вакансию приходится всего 0,8 резюме

Опрос hh.ru и Сёрчинформ

Факторы дефицита квалифицированных ИБ-кадров

Новый уровень кибреугроз

Добавились те, что исходят от профессиональных структур других государств — для нанесения прямого ущерба

Импортозамещение требует переобучения и сертификации

Требуются ИБ-специалисты новой формации, на новые стеки и ПО
Оценка компетенций

Необходимо менять модель подбора и удержания ИБ-специалистов

Качественный найм через обучение стажеров

Киберграмотность и киберэтика – приоритет номер один для инвестиций

Рост уровня цифровизации и автоматизации предприятий

Рост технологий связанных с аналитикой данных
Обязательства по защите персональных данных

Изменения на рынке труда

Рынок переполнен низкоквалифицированными кандидатами с навыками «войти в ИТ за 3 мес»
Узкий инженерный кругозор

Факторы роста рынка ИБ и кадрового дефицита

Продолжается рост числа кибератак на органы власти, бизнес и промышленные объекты экономики РФ

Замена освободившегося рынка мировых вендоров российскими производителями

Ответственность первых лиц организаций за обеспечение их информационной безопасности (Указ Президента от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ»)

С 31 марта 2022 года запрет закупки зарубежного программного обеспечения для использования на значимых объектах КИИ. С 1 января 2025 года запрещает использование зарубежного ПО на всех объектах, определенных Указом Президента № 250 (Указ Президента от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ»)

Стимулирование развития отрасли (субсидии и гранты, другие меры поддержки отрасли: налоговые и прочие льготы)

Ужесточаются требования отраслевых регуляторов, предъявляемые к заказчикам решений ИБ, что будет дополнительно стимулировать спрос

Оценка влияния факторов на рост рынка до 2027 года

Фактор	2023	2024	2025	2026	2027
Рост числа кибератак	8%	7%	6%	6%	6%
Уход зарубежных вендоров	7%	5%	3%	3%	3%
Санкции и связанные с ними ограничения	-2%	-2%	-2%	-1%	-1%
Ответственность первых лиц организаций за обеспечение ИБ	0%	0%	0%	0%	0%
Запрет зарубежного ПО на объектах КИИ	1%	1%	1%	0%	0%
Финансовые меры поддержки	10%	10%	10%	9%	9%
Нефинансовые меры поддержки	2%	2%	2%	2%	2%
Ужесточение требований к ИБ	-1%	-1%	-1%	-1%	-1%
Готовность заказчиков к импортозамещению	5%	10%	–	–	–
ИТОГОВЫЙ РОСТ РЫНКА (ГОД К ГОДУ)	31%	32%	19%	18%	18%

Источник: Центр стратегических разработок (ЦСР)

Прогноз развития рынка кибербезопасности России на 2023 – 2027 годы

Актуальные ИБ-компетенции для ОКИИ

Нормативно-правовое обеспечение и организационные меры информационной безопасности

- Управление ИБ
- Стратегическое планирование и управление
- Обеспечение ИБ
- Нормативно-правовое обеспечение ИБ
- Обучение и повышение квалификации

Мониторинг событий и реагирование на инциденты

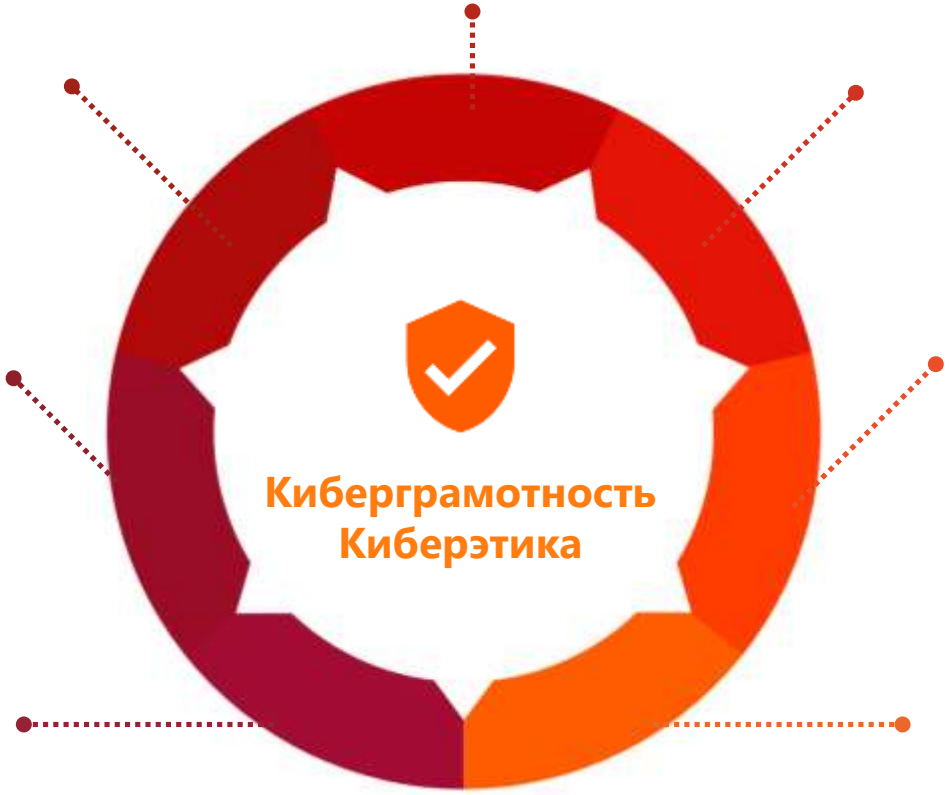
- Мониторинг событий
- Реагирование на инциденты
- Оценка и управление уязвимостями
- Поддержка инфраструктуры

Аналитика ИБ

- Анализ эксплуатации уязвимостей ИС
- Анализ данных из разных источников
- Прогнозирование угроз безопасности

Расследование компьютерных инцидентов

- Цифровая криминалистика
- Расследование компьютерных инцидентов



Сбор данных и эксплуатация уязвимостей ИС

- Сбор данных из разнородных источников
- Планирование реализаций мероприятий в области ИБ
- Создание и поддержка баз знаний по расследованию киберинцидентов

Эксплуатация и техническое обслуживание технических систем

- Системное администрирование
- Эксплуатация сетей
- Системный анализ
- Администрирование данных
- Обслуживание клиентов и техническая поддержка

Безопасная разработка

- Разработка ПО
- Управление рисками
- Архитектура корпоративных ИС
- Разработка ИС
- Тестирование и оценка ПО

академия softline

ПРОГРАММЫ ДПО И ОБРАЗОВАТЕЛЬНЫЕ РЕШЕНИЯ

Для подготовки ИБ-кадров и повышения киберграмотности для объектов КИИ

Профессиональная переподготовка

Информационная безопасность.
Обеспечение защиты информации ограниченного доступа,
не содержащей сведения, составляющие государственную тайну

Согласована со ФСТЭК

Включено 100+ часов обеспечения безопасности значимых объектов КИИ

Навыки и компетенции по результатам обучения:

- # Работать с нормативно-правовой и методической базой технической защиты информации
- # Проводить аттестации объектов информатизации на соответствие требованиям
- # Устанавливать, монтировать, испытывать и устранять неисправности средств технической защиты конфиденциальной информации
- # Выявлять угрозы безопасности по результатам оценки внешних и внутренних нарушителей
- # Мониторить защищенность конфиденциальной информации и отчитываться по результатам контроля
- # Разрабатывать организационно-распорядительные документы по безопасности значимых объектов

Для кого

01 

Руководителям и уполномоченным руководить работами по лицензируемому виду деятельности

02 

Специалистам субъекта критической информационной инфраструктуры, ответственным за обеспечение безопасности значимых объектов КИИ

03 

Специалистам (инженерно-техническим работникам) в области ТЗКИ от НСД

04

Специалистам (инженерно-техническим работникам) в области ТЗКИ от утечки по техническим каналам

Программа повышения квалификации (ФЗ-187)

Программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

Согласована со ФСТЭК

Навыки и компетенции по результатам обучения:

- # Проводить анализ и определять уровень опасности угрозы безопасности информации
- # Организовывать работу и обеспечивать выполнение требований законодательства в сфере обеспечения безопасности объектов КИИ187
- # Разбираться в вопросах категорирования объектов КИИ
- # Разрабатывать организационно-распорядительные и планирующие документы, регламентирующие безопасность значимых объектов КИИ
- # Реализовывать меры по обеспечению безопасности значимых объектов КИИ187
- # Реализовывать требования по взаимодействию с контролирующими органами
- # Реализовывать меры по контролю за обеспечением безопасности значимого объекта КИИ

Для кого

01 

Руководителям и сотрудникам государственных и муниципальных органов, органов местного самоуправления, организаций различных форм собственности

02 

Руководителям и специалистам служб ИБ и защиты информации государственных и коммерческих предприятий

03

Индивидуальным предпринимателям в областях информатизации, телекоммуникационных технологий, здравоохранения, науки, транспорта, связи, энергетики, банковской сферы и др.

Решение для обучения персонала значимых объектов КИИ

наша безопасность

На страже киберграмотности!

Платформа для повышения осведомленности специалистов значимых объектов КИИ в области информационной безопасности и защиты персональных данных

Обучение навыкам безопасного поведения

Подавляющая часть первопричин киберугроз и киберинцидентов имеет **человеческий фактор**, именно рядовые сотрудники компаний чаще являются прямыми или косвенными источниками «результативности» фишинговых атак, утечки данных, и иных инцидентов, приводящих к необратимым последствиям.

Решение под ключ

Образовательная платформа с курсами по повышению осведомленности

- Автоматизация обучения
- Удобная установка на сервер вашей компании или подписка на облачный сервис
- Брендирование под фирменный стиль заказчика
- Удобное управление и администрирование образовательного процесса
- Статистика и отчеты
- Бесплатная техническая поддержка 6 мес.

Обучение сотрудников распознаванию и предотвращению цифровых атак, защите персональных данных

Стажерская программа
Школа «ИБ-кадры»

1. **Обучение команд стажеров, кадрового резерва под задачи заказчика**

2. **Индивидуальные образовательные программы в соответствии с заданным технологическим стеком**

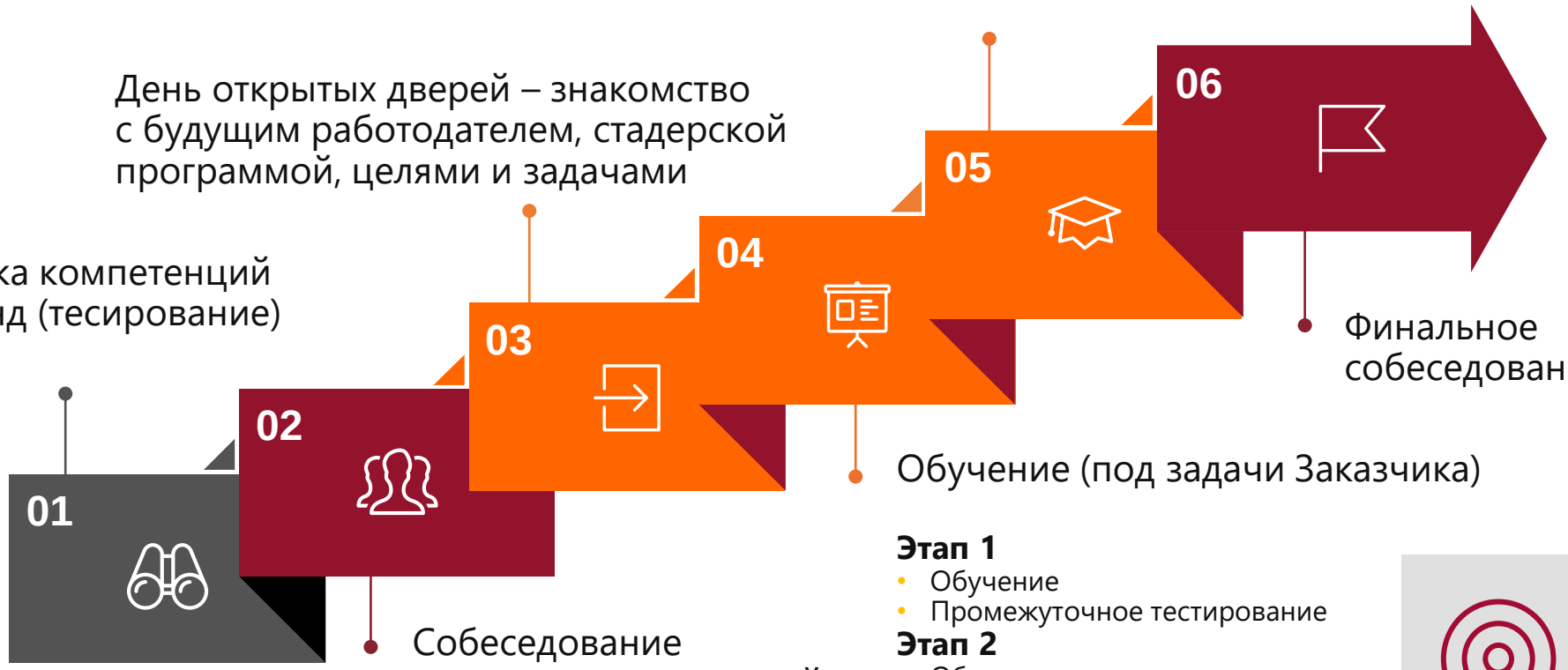
3. **Решение задач по оценке компетенций и повышения квалификации под набор компетенций**

4. **Оптимизация сроков подбора команд и бюджета на рекрутинг**

Решение для обучения стажеров по Информационной безопасности

Школа ИБ-кадры

Готовые кандидаты к приему в штат



Оценка компетенций команд (тесирование)

Собеседование кандидатов с командой Заказчика

День открытых дверей – знакомство с будущим работодателем, стадерской программой, целями и задачами

Обучение (под задачи Заказчика)

Этап 1
- Обучение
- Промежуточное тестирование

Этап 2
- Обучение
- Итоговое тестирование.

Финальное собеседование

Результат: сформированная команда в штат

академия softline

Спасибо за внимание

Через обучение - к успеху!
Знания работают на вас