Специалист по информационной безопасности

01 Кому подойдёт курс

Начинающим без опыта

Если вы только начинаете путь в информационной безопасности и не имеете технического опыта. Мы объясняем всё с нуля — без воды, с фокусом на практике и реальных навыках. Достаточно уметь пользоваться компьютером на базовом уровне — остальному мы научим.

Специалистам из смежных IT-сфер

Если вы работаете в системном администрировании, технической поддержке или других смежных отраслях и думаете о карьерном росте — курс поможет вам перейти в информационную безопасность, повысить квалификацию и получить структурированные знания. Вы сможете применять материал сразу в работе, а также подготовиться к переходу на новую должность или смене работы.

Студентам и выпускникам технических специальностей

Если вы учитесь в вузе или колледже, но чувствуете, что не хватает практики и актуальных навыков, на курсе вы сможете закрыть теоретические пробелы, попрактиковаться в навыках на виртуальных машинах и собрать портфолио, чтобы уверенно претендовать на стажировки и первые рабочие позиции в сфере кибербезопасности.

02 Какие знания и навыки освоите

- Администрирование сетей и настройка ОС (Windows и Linux) для повышения безопасности инфраструктуры;
- Написание скриптов на Bash и PowerShell;
- Установка и настройка средств защиты информации;
- Выявление причин падения систем и поддержание работоспособности инструментов;
+ Реализация безопасных решений согласно законодательным стандартам;
- Требования и особенности защиты инфраструктуры в востребованных отраслях: коммерция, финансы и государственные сервисы. *В расширенном тарифе

03 Как проходит обучение

- Теория и практика на платформе Практикума
- Каждый теоретический блок закрепляется практическим проектом
- Практические задания на виртуальных машинах в Яндекс.Облако
- Команда сопровождения будет помогать вам на протяжении всего обучения
- Онлайн-семинары для закрепления материала или разбора сложных моментов

Специалист по информационной безопасности

Что вас ждёт на обучении

Актуальные инструменты и подходы к защите инфраструктуры компании

Практика, основанная на решении реальных рабочих задач

Обучение от экспертов из Яндекса и других крупных компаний

01 В чём суть профессии

Специалист по информационной безопасности защищает компании от кибератак, утечек данных и внутренних угроз.

Он настраивает защиту, анализирует подозрительные события, реагирует на инциденты и помогает соблюдать законы по работе с данными.

Без него компания рискует потерять деньги, репутацию и доверие клиентов.

02 В каких сферах работают

Специалисты по информационной безопасности востребованы почти везде, где есть цифровые данные. Больше всего вакансий — в банках и финансовых организациях, госструктурах, IT-интеграторах и крупных корпорациях, где особенно важно защищать информацию от утечек и атак. Также СИБы работают в технологических компаниях, телекоммуникациях, энергетике и даже в стартапах — любая компания с данными и интернет-инфраструктурой нуждается в защите.

03 Какие задачи решают

Расследуют подозрительные события — например, если у сотрудника с рабочего компьютера внезапно начали скачиваться тысячи файлов, специалист по информационной безопасности проверит, не скомпрометирован ли аккаунт, и вовремя остановит утечку данных.

Настройка защиты для новых сервисов — когда компания запускает онлайн-сервис, специалист ИБ проверяет, как передаются данные, нет ли уязвимостей и не может ли злоумышленник получить доступ к персональной информации, если находит уязвимые места — предпринимает меры по защите инфраструктуры.

Обучают сотрудников безопасному поведению — например, проводят тесты на фишинг: рассылают «фиктивные» письма и смотрят, кто попадётся, чтобы потом объяснить, как распознавать настоящие атаки.

04 Карьерные перспективы

Из года в год интенсивность кибератак в мире продолжает расти. При этом со стороны государства растут штрафы за утечки персональных данных. Всё это порождает устойчивый спрос на квалифицированных специалистов по информационной безопасности. В связи с чем отрасль является одной из самых быстрорастущих.

Специалист по информационной безопасности

Сравнение тарифов

Названия оцениваемых критериев	Специалист по информационной безопасности	Специалист по информационной безопасности расширенный
Длительность	11 месяцев	13 месяцев
Каникулы	6 недель	7 недель
Нагрузка	от 15 часов в неделю	от 15 часов в неделю
Практика	На виртуальных машинах в Яндекс.Облако	На виртуальных машинах в Яндекс.Облако
Помощь в трудоустройстве	✓	✓
Вакансии и стажировки от партнёров	✓	✓
Сопровождение: наставник, преподаватель, ревьюеры, куратор, техподдержка	✓	✓
Вебинары	✓	✓ + Сессия вопросов и ответов с экспертом по информационной безопасности из Яндекса
Проекты в портфолио	4 проекта: 3 практических + 1 итоговый	6 проектов: 3 практических проекта + 3 бизнес-кейса от Яндекса из разных отраслей: финтех, государственные сервисы, коммерция
Итоговый проект	Выполняется самостоятельно	Выполняется самостоятельно + сопровождение от наставника в роли тимлида в режиме, приближенном к реальной работе

Преимущества расширенного курса

01 Больше практики

В базовом тарифе вы сможете выполнить 4 проекта в портфолио. Программа расширенного тарифа предлагает те же 3 практических проекта + 3 бизнес-кейса из востребованных отраслей (финансы, государственные сервисы, коммерция). Один из кейсов — итоговый проект.

Почему именно эти отрасли? Мы проанализировали рынок вакансий и выяснили, что более 50% позиций для начинающих специалистов ИБ сосредоточено в трёх сферах — финансы, государственные информационные системы и коммерческий сектор. Именно поэтому мы включили в программу расширенного тарифа три бизнес-кейса с реальной спецификой этих направлений. Так вы получите прикладной опыт в сферах и повысите свои шансы попасть на работу туда, где сейчас больше всего возможностей.

02 Сопровождение итогового проекта приближено к реальной работе

Как и в любом профессиональном обучении, и базовый, и расширенный тарифы включают итоговый проект. Но в расширенном тарифе вы пройдёте его в условиях, близких к реальной работе: вам будет выделен наставник, который выступит в роли тимлида — он будет ставить задачи, проверять решения и регулярно давать обратную связь. Такая модель помогает не просто сдать проект, а прочувствовать, как устроен процесс в настоящей ИБ-команде, и быстрее адаптироваться на первой работе.

03 Экспертиза Яндекса

Кейсы в тарифе созданы совместно с командой инженеров по информационной безопасности из разных департаментов Яндекса (Яндекс.Банк, Яндекс.Маркет, Яндекс.Облако) на основе их реального опыта. Эксперты вложили в материалы свои методологии, подходы и лучшие практики из работы. Вы будете учиться у тех, кто защищает одну из крупнейших IT-компаний России.

Вы также получите возможность поучаствовать в закрытой сессии вопросов и ответов с действующим ИБ-специалистом Яндекса — задать вопросы, узнать, как устроена работа изнутри, и перенять ценный опыт напрямую от профессионала.

Специалист по информационной безопасности

Базовый тариф

11 месяцев — продолжительность курса
4+ проекта в портфолио
20 воркшопов с наставником

Расширенный тариф

13 месяцев — продолжительность курса
4+ проекта в портфолио
20 воркшопов с наставником

Базовый тариф

Факультативный курс	Подготовительный блок. Основы знаний о компьютере	1 неделя / 15 часов
Модуль 1. Настройка корпоративных ИТ-сервисов в среде эмуляции	Спринт 1. Настройка локальной корпоративной сети в эмуляторе	2 недели / 30 часов
	Спринт 2. Настройка операционной системы	2 недели / 30 часов
	Спринт 3. Развёртывание инфраструктурных сервисов	2 недели / 30 часов
	Спринт 4. Запуск прикладных сервисов с корректировкой конфигурации	2 недели / 30 часов
	Спринт 5. Проектная работа №1	2 недели / 30 часов
	Каникулы	2 недели
Модуль 2. Обеспечение безопасности корпоративных сервисов	Спринт 6. Моделирование угроз	2 недели / 30 часов
	Спринт 7. Сетевая безопасность веб-приложений	2 недели / 30 часов
	Спринт 8. Безопасность входящей электронной почты	2 недели / 30 часов
	Каникулы	1 неделя
	Спринт 9. Безопасность конечных устройств	2 недели / 30 часов
	Спринт 10. Безопасность корпоративной сети	2 недели / 30 часов
	Спринт 11. Выявление угроз и внедрение требуемого средства защиты	2 недели / 30 часов
	Спринт 12. Проектная работа №2	2 недели / 30 часов

Специалист по информационной безопасности

Базовый тариф

Модуль 3. Администрирование, поддержка и устранение неисправностей средств защиты информации	Спринт 13. Администрирование и поддержка средств защиты	2 недели / 30 часов
	Спринт 14. Регистрация событий: расследование инцидентов, поиск и устранение неисправностей (траблшутинг)	2 недели / 30 часов
	Спринт 15. Проектная работа №3	2 недели / 30 часов
	Каникулы	2 недели
Модуль 4. Разработка и внедрение политик безопасности	Спринт 16. Применение требований стандартов	2 недели / 30 часов
	Спринт 17. Поиск альтернативных решений	2 недели / 30 часов
Модуль 5. Виртуализация и контейнеризация	Спринт 18. Виртуализация и контейнеризация	2 недели / 30 часов
	Каникулы	1 неделя
	Итоговый проект базового тарифа	2 недели/30 часов

Расширенный тариф*

*Первые 18 спринтов Расширенного курса полностью совпадают с Базовым.

Модуль 6. Защита современных информационных систем	Спринт 19. Как защитить гос.систему и привести её в соответствие с требованиями регулятора	2 недели / 30 часов
	Спринт 20. Комплексный кейс: Расследование инцидента взлома государственной информационной системы «ГосСервис»	2 недели / 30 часов
Модуль 7. Защита информации в банковской сфере	Спринт 21. Как защитить банк и его клиентов	2 недели / 30 часов
	Спринт 22. Комплексный кейс: «Проведение аудита системы защиты банка»	2 недели / 30 часов
	Каникулы	1 неделя
	Итоговый проектный месяц	2 недели / 30 часов

Преридинг

00

1 неделя | 15 часов

факультативный курс

В этом блоке мы рассказываем о базовых принципах работы компьютера. Блок необязателен для прохождения, однако пройдя его, вы будете увереннее чувствовать себя в начале обучения.

Содержание

Основы знаний о компьютере

Темы

1. Как работает компьютер
2. Выход в сеть: от домашнего роутера до космического спутника

Настройка корпоративных ИТ-сервисов в среде эмуляции 01

12 недель | 180 часов

Настроите корпоративную сеть с почтой, веб-порталом, файловым сервером и инфраструктурными сервисами в эмуляторе

Содержание

Спринт 1. 2 недели	Настройка локальной корпоративной сети в эмуляторе	**Темы** 1. Введение в сети 2. Сетевые технологии 3. Администрирование сети	**Практика** Проектирование и настройка локальной корпоративной сети в эмуляторе для двух отделов компании и серверной комнаты **Вебинар** Разбор кейсов с наставником
Спринт 2. 2 недели	Настройка операционной системы	**Темы** 1. Основы операционных систем 2. Linux 3. Windows	**Практика** Подготовка отчёта по реализации мониторинга **Вебинар** Разбор файлов с помощью bash-скриптов
Спринт 3. 2 недели	Развёртывание инфраструктурных сервисов	**Темы** 1. Возвращаемся к сетевым моделям 2. Настраиваем DNS и NTP 3. Централизованное управление 4. Резервное копирование	**Практика** Развёртывание инфраструктурных сервисов в сети компании «Вокруг света» **Вебинар** Инфраструктура доступа Active Directory
Спринт 4. 2 недели	Запуск прикладных сервисов с корректировкой конфигурации	**Темы** 1. Введение в прикладные сервисы 2. Электронная почта 3. Веб-ресурсы 4. Файловые серверы	**Практика** Запуск прикладных сервисов с корректировкой конфигурации для стартапа CloudSecure **Вебинар** Маршрут доставки электронных писем
Спринт 5. 2 недели	Проектная работа №1	**Настройка корпоративной сети** Настроите корпоративную сеть с основными бизнес-сервисами (почта, веб-порталом, файловый сервер) и инфраструктурными сервисами в эмуляторе, наладите мониторинг работоспособности сервера **Проект**	

Обеспечение безопасности корпоративных сервисов 02

14 недель | 210 часов

Выявите и оцените актуальные угрозы корпоративной сети. Внедрите средства защиты информации, которые требуются, чтобы нейтрализовать выявленные угрозы

Содержание

Спринт 6. 2 недели	Моделирование угроз	**Темы** 1. Бизнес-процессы компании 2. Выявление рисков 3. Моделирование угроз	**Практика** Моделирование угроз в кейсе «ИнвестПро» **Вебинар** Оценка рисков информационной безопасности
Спринт 7. 2 недели	Сетевая безопасность веб-приложений	**Темы** 1. Атака как цепочка событий 2. Атаки на Веб-приложения 3. Устранение уязвимостей веб-приложений 4. Web Application Firewall	**Практика** Поиск и устранение уязвимостей в приложении «Сок и фрукты» **Вебинар** Синергия атаки и защиты. Почему важно знать всё про обе стороны
Спринт 8. 2 недели	Безопасность входящей электронной почты	**Темы** 1. Почта как точка входа в инфраструктуру 2. Атаки на почту 3. Выявление вредоносных рассылок 4. ESG	**Практика** Оценка эффективности фильтров почтового сервера для компании «СосныИзЛеса» **Вебинар** Социальная инженерия и фишинговые письма
Спринт 9. 2 недели	Безопасность конечных устройств	**Темы** 1. Векторы атак на endpoint 2. Продвинутые атаки на эндпоинты 3. Повышение защищённости ОС (харденинг ОС- от англ. «hardening») 4. Средства защиты информации конечных устройств	**Практика** Анализ и устранение уязвимостей в инфраструктуре Active Directory нового подразделения компании. **Вебинар** Харденинг и безопасность конечных узлов
Спринт 10. 2 недели	Безопасность корпоративной сети	**Темы** 1. Сетевая безопасность и виды атак 2. Повышение защищённости сети (харденинг сети - от англ. «hardening») 3. Средства защиты сети, обнаружение и предотвращение сетевых атак	**Практика** Проектирование и реализация сегментированной инфраструктуры с политикой сетевого доступа **Сессия** Вопросы и ответы с наставником

Содержание

Спринт 11. 2 недели	Выявление угроз и внедрение требуемого средства защиты	**Темы** 1. Безопасность компании «Всем по даркстору» 2. Безопасность компании «Вайб-кодинг»	**Практика** Поиск и устранение уязвимостей в компании «Всем по даркстору» **Вебинар** Эксплуатация уязвимостей
Спринт 12. 2 недели	Проектная работа №2	**Анализ бизнес-процессов компании, оценка угроз и внедрение мер безопасности** Проанализируете бизнес-процессы компании, оцените угрозы и внедрите необходимые средства защиты информации и меры безопасности **Проект**	

Администрирование, поддержка и устранение неисправностей средств защиты информации 03

6 недель | 90 часов

Изучите полный цикл администрирования и поддержки средств защиты - от выполнения рутинных задач по настройке и поддержке до решения проблем работоспособности самого средства или бизнес-сервисов.

Содержание

Спринт 13. 2 недели	Администрирование и поддержка средств защиты	**Темы** 1. Администрирование СЗИ и задачи специалистов 2. Жизненный цикл сервиса информационной безопасности 3. Как управлять изменениями в сервисе информационной безопасности	**Практика** Администрирование и поддержка средств защиты на примере антивирусного ПО **Вебинар** Аудит коммуникации: команда ИБ в действии
Спринт 14. 2 недели	Регистрация событий: расследование инцидентов, поиск и устранение неисправностей (траблшутинг)	**Темы** 1. Логирование событий 2. Расследование инцидентов 3. Устранение аварий в инфраструктуре	**Практика** Расследование инцидента ИБ в компании «Сфера Логистикс» **Вебинар** Устранение аварии
Спринт 15. 2 недели	Проектная работа №3	**Поддержка средства защиты** Решите несколько обращений пользователей и IT-специалистов корпоративной сети, выявите причины, по которым возникают разные типы аварий и ошибок конфигурирования и их природу. **Проект**	

Разработка и внедрение политик безопасности

04

4 недели | 60 часов

Оцените, насколько применимы требования в стандарте. Если требования неприменимы - предложите альтернативное решение.

Содержание

Спринт 16.
2 недели

Применение требований стандартов

Темы

1. Как появляются правила информационной безопасности
2. Стандарты и как оценить их на применимость и релевантность
3. Применяем стандарты и устраняем несоответствия

Практика

Применение требований стандартов для компании «Сделали Софт»

Вебинар

Применение требований стандартов

Спринт 17.
2 недели

Поиск альтернативных решений

Темы

1. Первичный анализ
2. Как использовать уже существующие стандарты
3. Написание корпоративного стандарта

Практика

Разработка стандарта безопасной настройки инфраструктуры для компании «Полёт»

Вебинар

Сессия Вопросы и ответы с наставником

Виртуализация и контейнеризация

05

1 неделя | 15 часов

Узнаете, как используется виртуализация и контейнеризация в корпоративных сетях.

Содержание

Спринт 18.
1 неделя

Виртуализация и контейнеризация

Темы

1. Виртуализация
2. Контейнеризация

Практика

Создание своей контейнерной лаборатории для обучения

Вебинар

Применение требований стандартов

Защита современных информационных систем 06

4 недели | 60 часов

Оцените, насколько применимы требования в стандарте. Если требования неприменимы — предложите альтернативное решение.

Содержание

Спринт 19.
2 недели

Как защитить госсистему и привести её в соответствие с требованиями регулятора

Темы

1. Архитектура ГИС. Контекст и угрозы
2. Защита периметра ГИС и инфраструктуры
3. Обеспечение соответствия требованиям регулятора
4. Оценка соответствия системы требованиям регулятора и подготовка отчёта

Практика

Аудит виртуальной ГИС «ГосТест» по чек-листу регулятора и подбор релевантных задаче решений

Вебинар

Особенности защиты современных государственных систем от эксперта отрасли

Спринт 20.
2 недели

Комплексный кейс. Расследование инцидента взлома государственной информационной системы «ГосСервис».

По инфраструктуре и событиям восстановите ход атаки и переведёте его в понятный для руководства и регуляторов план доработок, чтобы защитить бизнес и выполнить требования по защите ГИС.

Проект

Защита информации в банковской сфере 07

4 недели | 60 часов

Разберётесь, как работают банковские информационные системы и какие уязвимости делают их мишенью для киберпреступников. Изучите требования отраслевого регулятора для определения уровня защиты банка, требования Центрального Банка и познакомитесь с современными средствами защиты.

Содержание

Спринт 21. 1 неделя	Как защитить банк и его клиентов	**Темы** 1. Введение в информационную безопасность финтеха 2. Нормативная база финтеха — ГОСТ Р 57580 3. Стандарты Центрального Банка и международный стандарт 4. Подходы к защите клиентов. Мультифакторная аутентификация (MFA) для банков 5. Принципы сегментации и зонирования в банковских сетях **Практика** Защита учётных записей и сети в виртуальном банке MiniBank, применение MFA и принципов сегментации и зонирования **Вебинар** Особенности защиты информации в банковской сфере от эксперта отрасли
Спринт 22. 2 недели	Комплексный кейс. Проведение аудита системы защиты банка.	Проанализируете систему защиты банка, разработаете и внедрите план по устранению выявленных рисков, протетстируете решение и по итогу оформите отчёт для руководства. **Проект**

Итоговый проектный месяц 08

3 недели | 45 часов

В рамках проектного месяца погрузитесь в сферу электронной коммерции. Настроите систему защиты онлайн-магазина в соответствии с бизнес-требованиями и стандартами. Пройдете все шаги - от аудита и внедрения СЗИ до тестирования и формирования внутреннего отчета

Медведев Кирилл
Директор АНО ДПО «Образовательные технологии Яндекса»

Автономная некоммерческая организация дополнительного профессионального образования ★ МОСКВА ★ ОГРН 1147799006123 «Образовательные технологии Яндекса» Yandex EdTech