Онлайн-практикум по кибербезопасности: решаем задание CTF за три дня

Практикуемся на задачах с соревнований CTF под руководством эксперта

Эксперт по кибербезопасности Павел Блинников

- Глава российской команды SPRUSH
- 7 лет опыта участия в CTF
- 3 года работы в цифровой криминалистике

Прием-прием

SkillFactory

Поставьте в чат +,
если хорошо слышно и видно

Ведущая

SkillFactory

Виктория Платунова

Создаю бесплатные мероприятия по Data Science в Skillfactory

Высшее образование по направлению управление персоналом, но строю карьеру в маркетинге, поэтому не понаслышке знаю о кардинальной смене деятельности

SkillFactory

Подарки для участников практикума

скидка 45% на покупку обучения от МИФИ x Skillfactory

Курс Базовый SQL победителям, которые наберут 2.500 очков по итогам нашего CTF

Добавляйтесь в наш телегр
чат практикума

Он будет действовать три дня.

Там вы сможете задать вопросы эксперту,
обменяться впечатлениями.

</>

SkillFactory

Онлайн-обучение от SkillFactory и НИЯУ МИФИ «Информационная безопасность»

- 10 месяцев обучения
- 4 проекта в портфолио
- Помощь в трудоустройстве от нашего Центра карьеры
- Беспроцентная рассрочка с ежемесячным платежом за курс

– 45%

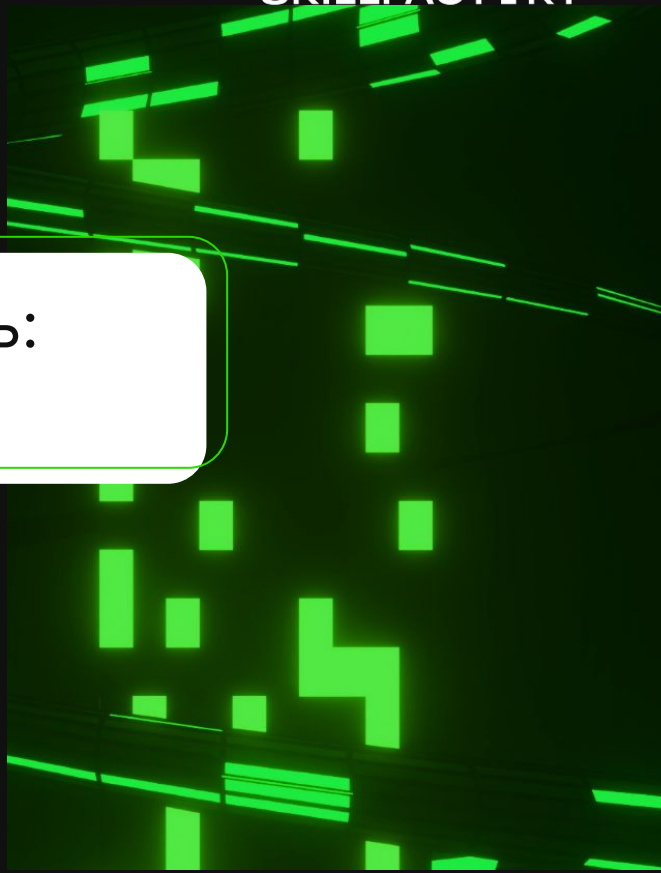
на обучение для участников практикума

Чтобы закрепить за собой предложение, **нужно оставить заявку**: нажать кнопку возле экрана, перейти и за 1 минуту оставить свои контакты

SKILLFACTORY

Онлайн-магистратура Skillfactory x МИФИ

Информационная безопасность: пентест и комплаенс



- 2 года обучения
- Диплом магистра МИФИ
- Помощь в трудоустройстве от Центра карьеры

Как проходит обучение на программе:

SKILLFACTORY

Индивидуальная работа

Видеолекции, презентации, конспекты, домашние задания и онлайн-тренажеры на платформе. Персональные проекты, общение с координатором, практики и стажировки

Как проходит обучение на программе:

SKILLFACTORY

Индивидуальная работа

Видеолекции, презентации, конспекты, домашние задания и онлайн-тренажеры на платформе. Персональные проекты, общение с координатором, практики и стажировки

Групповая работа

Проекты в команде, соревнования, обмен опытом

Как проходит обучение на программе:

SKILLFACTORY

Индивидуальная работа

Видеолекции, презентации, конспекты, домашние задания и онлайн-тренажеры на платформе. Персональные проекты, общение с координатором, практики и стажировки

Групповая работа

Проекты в команде, соревнования, обмен опытом

В синхронном режиме

Онлайн-лекции, семинарские занятия, гостевые лекции, индивидуальные консультации (Zoom, вебинары)

SKILLFACTORY

Магистратура vs онлайн-магистратура

Сходства

- Обучение разбито на 4 семестра, каждый завершается сессией
- Между семестрами есть каникулы (в том числе двухмесячные летние)
- Отдых в государственные праздничные дни
- Вступительные испытания
- Необходимо подготовить и сдать выпускную квалификационную работу
- Программа соответствует федеральным образовательным стандартам

Различия

- Можно учиться, находясь в любой точке мира, нет обязательных очных мероприятий
- Большое количество практики, стажировок и обмена опытом с экспертами благодаря независимости от местоположения

Наш диплом — первая строчка в вашем резюме

SKILLFACTORY

Диплом магистра от НИЯУ МИФИ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ДИПЛОМ МАГИСТРА

ДОКУМЕНТ ОБ ОБРАЗОВАНИИ И О КВАЛИФИКАЦИИ

Регистрационный номер

Дата выдачи

Настоящий диплом свидетельствует о том, что

освоил(а) программу магистратуры по направлению подготовки

и успешно прошел(ла) государственную итоговую аттестацию

Решением Государственной экзаменационной комиссии присвоена(ы) квалификация(и)

Руководитель организации, осуществляющей образовательную деятельность

М.П.

Миф или правда?

Чтобы поступить в магистратуру МИФИ,
нужно иметь техническое образование.

SKILLFACTORY

Миф или правда?

~~Чтобы поступить в магистратуру МИФИ, нужно иметь техническое образование.~~

Чтобы поступить в магистратуру, нужно иметь диплом о высшем образовании и справиться с вступительным испытанием.

Можно ли совмещать очное обучение в онлайн-магистратуре с работой full-time?

SKILLFACTORY

Онлайн-занятия проходят по вечерам и в выходные. Даже в случае пропуска вы сможете посмотреть запись и наверстать упущенное. Главное — уделять достаточно времени самостоятельной работе.

В среднем 74% наших студентов работают полный день.

Вместе с HR-специалистами вы:

- Проведете аудит компетенций, определите цели и составите пошаговый план действий
- Составите резюме и портфолио, потренируетесь перед собеседованиями и тестовыми заданиями
- А еще первыми увидите вакансии от партнеров, поучаствуйте в активностях карьерного клуба, выстроите нетворкинг в закрытых каналах и чатах

Уже во время учебы сможете брать заказы на фрилансе, а с середины курса — откликаться на junior-вакансии

SkillFactory

Онлайн-обучение от SkillFactory и НИЯУ МИФИ «Информационная безопасность»

- 10 месяцев обучения
- 4 проекта в портфолио
- Помощь в трудоустройстве от нашего Центра карьеры
- Беспроцентная рассрочка с ежемесячным платежом за курс

6684 ₽

в месяц по беспроцентной рассрочке на 24 мес

Чтобы закрепить за собой предложение, **нужно оставить заявку**:
нажать кнопку возле экрана, перейти
и за 1 минуту оставить свои контакты

Информационная безопасность: пентест и комплаенс

SKILLFACTORY

- 2 года обучения
- Диплом магистра от НИЯУ МИФИ
- Помощь в трудоустройстве от Центра карьеры

Станьте востребованным специалистом в IT: отражайте кибератаки, защищайте данные пользователей и помогайте бизнесу

Начните работать по специальности уже через 7 месяцев обучения

Полная стоимость — 175 000 ₽ за семестр
700 000 ₽ за 2 года

- Государственный кредит на образование под 3%
- Возможность сделать налоговый вычет

Оставляйте заявку на консультацию, **чтобы закрепить за собой место в магистратуре** и узнать все подробности о программе и профессии

Эксперт

SkillFactory

ПАВЕЛ БЛИННИКОВ

- Глава российской команды SPRUSH
- 7 лет опыта участия в CTF
- 3 года работы в цифровой криминалистике

2 день

- История криптографии: шифры древности и Средневековья.
- Шифры 20 века: симметричное и асимметричное шифрование.
- Криптоанализ RSA

Криптография

Скитала

Atbash

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Шифр Цезаря (one byte XOR)

Последовательно сдвигаем каждую букву в тексте на констатный сдвиг по алфавиту. Например при сдвиге 4:

a → d

b → e

z → c

Шифр Виженера (XOR with key)

Складываем последовательно буквы в тексте с буквами в ключе. Неуязвимо если длина ключа равна длине шифруемого текста. Тогда такой шифр называется One-time pad.

мама + раму = эбщф

м (13) + р (17) = э (30)

а (1) + а (1) = б (2)

м (13) + м (13) = щ (26)

а (1) + у (20) = ф (21)

Небольшое отступление

Бит - единица информации, которая уменьшает неопределенность в 2 раза

Байт = 8 бит (2^8 = 256 различных комбинаций)

Кодировки (в классической вариации):
UTF-8 (1 байт - 1 символ)
UTF16 - (2 байта - 1 символ)

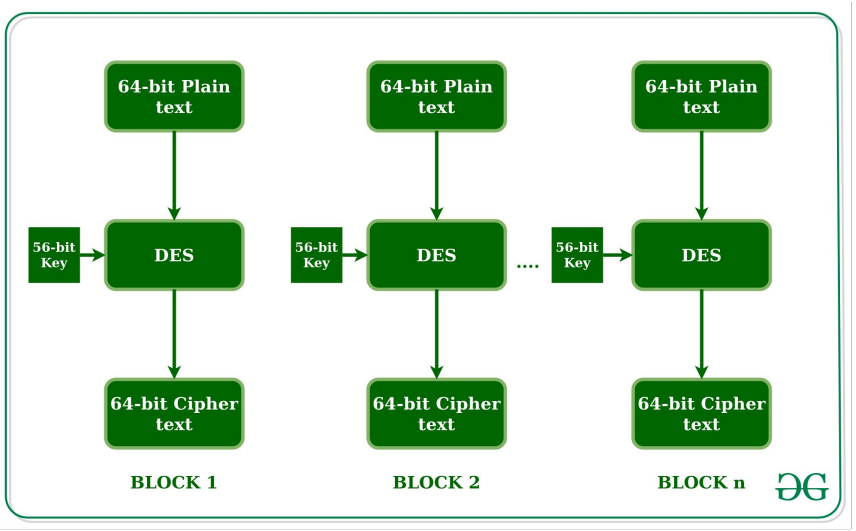
Типы шифрования

Симметричное шифрование: шифрование и расшифрование происходит одним и тем же ключом

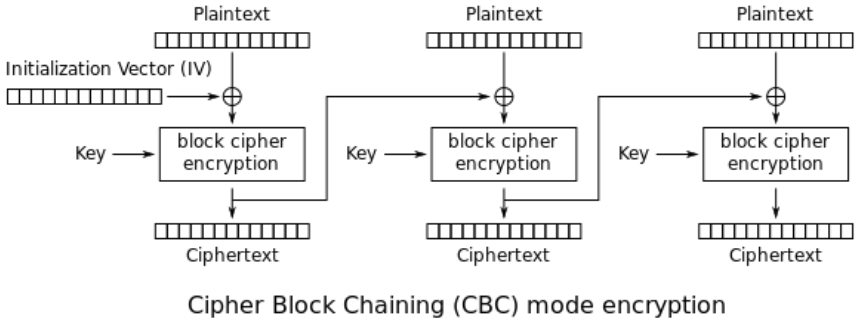
Асимметричное шифрование: шифрование и расшифрование происходит разными ключами. Публичным и приватным соответственно.

Пример симметричного шифрования

DES



AES



Cipher Block Chaining (CBC) mode encryption

Пример кода на Python

```
from Crypto.Cipher import AES

key = b'Sixteen byte key'

cipher = AES.new(key, AES.MODE_ECB)

ciphertext = cipher.encrypt(b“some text 16byte”)

print(ciphertext)
```

Функция Эйлера

Функция, результат который равен количеству взаимно простых чисел меньше или равных аргументу.

Например для числа 36: (1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35).
Поэтому phi(36) = 12

Для любого простого числа n: phi(n) = n - 1

RSA

Выбираем взаимно простые p и q. n = p*q

Вычисляем функцию Эйлера от n, которая в этом случае равна

phi = (p - 1) * (q - 1)

Выбираем e взаимно простое с phi

Считаем d, обратное к e в кольце по модулю phi

(e,n) - открытый ключ

(d,n) - закрытый ключ

Что проверять первым делом?

factordb.com

Метод факторизации Ферма

1. Извлекаем квадратный корень из n
2. Двигаемся относительно этого числа в меньшую (p) и большую (q) сторону, перемножая
3. Если p*q == n, то мы успешно факторизовали n

Взлом через малую открытую экспоненту

При малом e и количестве переданных шифротекстов k >= e можно провести дешифрацию с помощью атаки Хастада.

Эту атаку можно доказать с помощью китайской теоремы об остатках, но здесь мы этого делать не будем.

SkillFactory

Отвечаем на ваши вопросы

Учебный план

SKILLFACTORY

1 семестр

Цель семестра: освоите необходимую базу и сможете определиться с дальнейшим направлением — бумажная или техническая безопасность / Compliance vs Pentest. Получите опыт работы над первой задачей в сфере ИБ

Обязательные дисциплины:

- **Нормативное обеспечение информационной безопасности (зачет)**
- **Сети и системы передачи данных (зачет)**
- **Защита в операционных системах (зачет)**
- **Криптография (зачет)**
- **Технические средства защиты информации (экзамен)**
- Программная инженерия (экзамен)
- Теоретические основы информационной безопасности (экзамен)
- Защищенные информационные системы (экзамен)

Учебный план

SKILLFACTORY

2 семестр

Цель семестра: начнете углубляться в выбранное направление.
Попрактикуетесь в решении реальных бизнес-кейсов
в сфере аудита или пентеста и начнете работу над собственным проектом в рамках магистратуры

Обязательные дисциплины:

- Управление информационной безопасностью (зачет)
- Разработка защищенных программных систем (зачет)
- Технология построения защищенных автоматизированных систем (зачет)
- Мониторинг, аналитика и оценка рисков ИБ (экзамен)

Учебный план

SKILLFACTORY

2 семестр

Дисциплины по выбору:

Правовое обеспечение ИБ / Безопасность вычислительных сетей

Международные стандарты защиты информации / Выявление уязвимостей (сканеры, MBSA)

Аудит информационной безопасности / Системы мониторинга и управления инцидентами

Факультативные дисциплины:

Аттестация, сертификация, лицензирование

Защита персональных данных

Инструменты:
SIEM, SOC, MITRE ATT&CK, Nessus, Wireshark, Suricate, NIST

Учебный план

SKILLFACTORY

3 семестр

Цель семестра: выберете подходящие для своих целей и профессиональной траектории элективы для углубленного понимания и получения высокой экспертизы в контексте выбранной специализации. Проведете исследование и защитите MPV дипломного проекта в рамках магистратуры

Обязательные дисциплины:

Формализованные модели и методы решения аналитических задач (экзамен)

Искусственный интеллект в информационной безопасности (зачет)

Компьютерная криминалистика (экзамен)

Учебный план

SKILLFACTORY

3 семестр

Дисциплины по выбору:

Методы и средства защиты информации в системах электронного документооборота / Защита каналов связи

Информационно-аналитические системы защиты информации / Технологии противодействия компьютерным атакам

Экономическая безопасность/ Радиотелекоммуникационные сети и защита информации

Основы гражданского права и гражданского процесса / Технологии пентестинга, атаки и уязвимости

Факультативные дисциплины:

Защита КИИ (организационные и технические меры)

Обеспечение ИБ АСУ ТП

Инструменты:
ChatGPT, Forensics, VPN, Kali Linux, Metasploit

Учебный план

SKILLFACTORY

4 семестр

Цель семестра: систематизировать полученные знания и навыки для реализации карьерных целей, финализации и защиты итогового проекта магистратуры

Обязательные дисциплины:

Оценка эффективности проектов (экзамен)

Факультативные дисциплины:

Социальная инженерия

SKILLFACTORY

Академический директор программы — Ирина Подборская

- Руководитель направления обеспечения информационной безопасности внутренних активов АО «РУСАЛ Менеджмент», в ИБ с 2005 года

- Эксперт в области защиты персональных данных, тайн, критической информационной инфраструктуры

- Пишет кандидатскую диссертацию на тему «Создание методики и автоматизации процесса реагирования на компьютерные инциденты».

SkillFactory

Онлайн-обучение от SkillFactory и НИЯУ МИФИ «Информационная безопасность»

- 10 месяцев обучения
- 4 проекта в портфолио
- Помощь в трудоустройстве от нашего Центра карьеры
- Беспроцентная рассрочка с ежемесячным платежом за курс

6684 ₽

в месяц по беспроцентной рассрочке на 24 мес

Чтобы закрепить за собой предложение, **нужно оставить заявку**:
нажать кнопку возле экрана, перейти
и за 1 минуту оставить свои контакты

Информационная безопасность: пентест и комплаенс

SKILLFACTORY

- 2 года обучения
- Диплом магистра от НИЯУ МИФИ
- Помощь в трудоустройстве от Центра карьеры

Станьте востребованным специалистом в IT: отражайте кибератаки, защищайте данные пользователей и помогайте бизнесу

Начните работать по специальности уже через 7 месяцев обучения

Полная стоимость — 175 000 ₽ за семестр
700 000 ₽ за 2 года

- Государственный кредит на образование под 3%
- Возможность сделать налоговый вычет

Оставляйте заявку на консультацию, **чтобы закрепить за собой место в магистратуре** и узнать все подробности о программе и профессии

Спасибо, что были с нами!

Встречаемся завтра в 19:00 по мск
и продолжаем практиковаться