Нормативное обеспечение кибербезопасности

Оксана Докучаева
Академический руководитель дисциплины

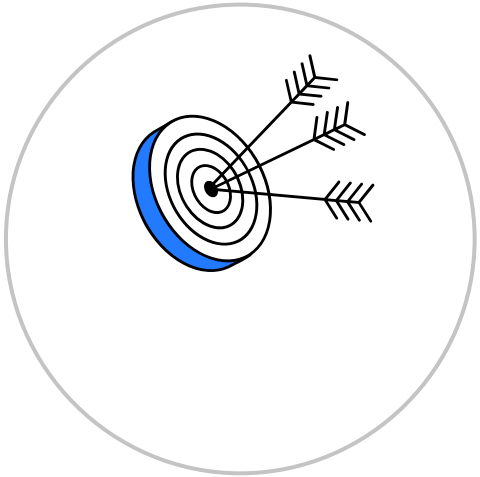
Приветствие

Дорогие студенты, рады видеть вас на дисциплине «Нормативное обеспечение кибербезопасности»

Вас ждет интересный, полный открытий, но порой требующий усилий путь. Мы поможем его пройти, поддержим в сложные моменты. Верим в ваш успех

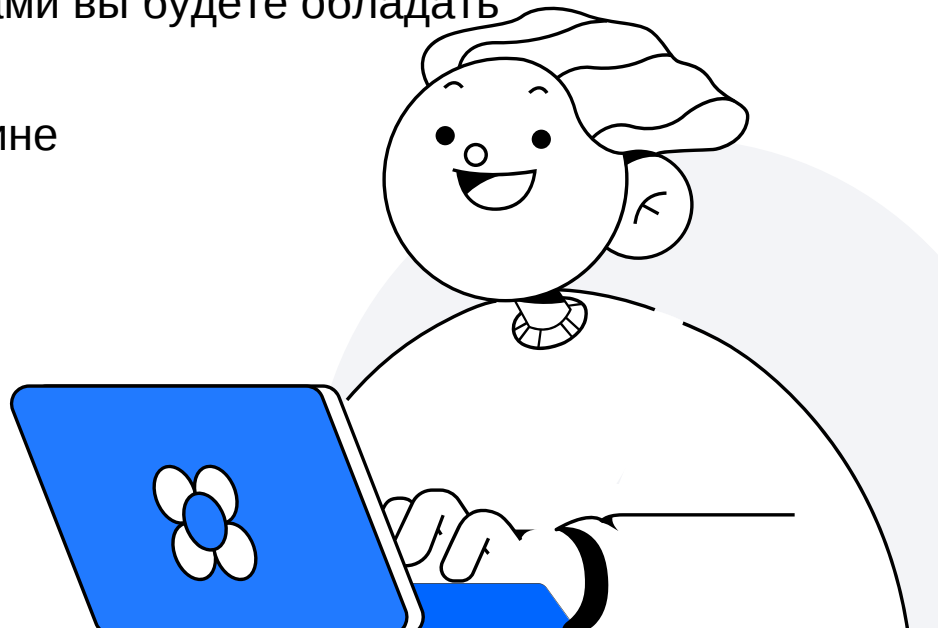
Вперед!

Ниже вы можете ознакомиться со всей важной информацией о курсе



Вы узнаете

1. Преподавателей-экспертов дисциплины
2. В какой последовательности изучать дисциплину
3. Какими знаниями, умениями и навыками вы будете обладать
4. Как получить аттестацию по дисциплине



Оксана Докучаева

О спикере:

- 14 лет оперативного опыта в Центре информационной безопасности ФСБ России
- Автор публикаций по информационной безопасности и расследованию компьютерных преступлений
- Опыт взаимодействия с Советом Безопасности РФ, правоохранительными органами, спецслужбами, организациями РФ в иностранных государствах по вопросам обеспечения информационной безопасности

Алексей Мунтян

О спикере:

- Основатель и CEO в компании Privacy Advocates
- Соучредитель в Russian Privacy Professionals Association (RPPA.ru)
- Внешний Data Protection Officer в четырех транснациональных холдингах
- Сопредседатель Privacy & Legal Innovation кластера РАЭК
- Участник центров компетенций «Информационная безопасность» и «Нормативное регулирование» при АНО «Цифровая экономика»
- Участник комитета по безопасности данных партнёров и пользователей при Консультативном совете по развитию экосистемы Яндекса

Павел Новожилов

О спикере:

- 13 лет в сфере ИБ
- Тимлид команды в области различных регуляторных требований
- Более 60 выполненных проектов
- Основные направления: ФЗ-152, ФЗ-187 и различные подзаконные акты, 638-П/747-П/719-П/716-П, стандарт ГОСТ 57580.1-2017, ISO 27001

Илья Воложанин

О спикере:

- Руководитель группы консалтинга
- Практикующий аудитор в области PCI DSS (7 лет)
- Общий опыт в области информационной безопасности — 15 лет
- QSA, CISSP, CISA

Аскар Мусаев

О спикере:

- Консультант по информационной безопасности
- Эксперт в области непрерывности бизнеса
- Опыт в информационной безопасности и непрерывности бизнеса более 6 лет
- Управлял и модернизировал системы управления непрерывностью бизнеса в ведущих компаниях, как в роли внутреннего специалиста, так и в качестве приглашенного эксперта
- Профессиональные сертификаты:
  ISO 22301-2019 Lead Auditor

Елена Агеева

О спикере:

- Ведущий консультант по информационной безопасности
- Общий опыт в области информационной безопасности — более 6 лет
- Основные направления работы: оценка рисков ИБ, защита от утечек конфиденциальной информации, защита персональных данных и коммерческой тайны, экспертный консалтинг ИБ

Александр Морковчин

О спикере:

- Руководитель группы департамента консалтинга центра информационной безопасности компании «Инфосистемы Джет»
- Более 10 лет работы в области информационной безопасности
- Основные направления в информационной безопасности — сложные комплексные проекты
- Международные сертификаты: CISSP, CISA, CISM, PCI DSS QSA

Структура курса (1 модуль, 114 академ. часа (3 ЗЕ**))

Эксперт: Оксана Докучаева

№	Тема	Видеолекций (академ. час)**	Часов вебинаров (академ.час)**	Академ. час. самост. работы, выполнения ДЗ
1	Введение в кибербезопасность	1	2	8
2	Нормативное регулирование информационной безопасности	2	4	17
3	Режимы информации ограниченного доступа	2	2	11
4	Классификация и категорирование информации, информационных систем	1	2	8
5	Лицензирование и сертификация. Сертификация и аккредитация	2	4	18
6	Правонарушения в сфере компьютерной информации	4	4	22

*ЗЕ - зачётная единица (1 ЗЕ=38 ак.часов) **1 академ.час = 45 мин.

Структура курса (2 модуль, 114 академ. часа (3 ЗЕ**))

№	Тема	Эксперт	Видеолекций (академ. час)**	Часов вебинаров (академ.час)**	Академ. час. самост. работы, выполнения ДЗ
1	Международные и отраслевые стандарты. GDPR	Алексей Мунтян		4	11
2	Международные и отраслевые стандарты. ISO 27001	Павел Новожилов	2	4	17
3	Международные и отраслевые стандарты. PCI DSS	Илья Воложанин	2	2	11
4	Международные и отраслевые стандарты. ISO 22301	Аскар Мусаев	1	2	8

*ЗЕ - зачётная единица (1 ЗЕ=38 ак.часов) **1 академ.час = 40 мин.

Структура курса (2 модуль, 114 академ. часа (3 ЗЕ**))

№	Тема	Эксперт	Видеолекций (академ. час)**	Часов вебинаров (академ.час)**	Академ. час. самост. работы, выполнения ДЗ
5	Управление рисками	Елена Агеева	1	4	15
6	Организация безопасности внутри компании. Ключевые аспекты построения системы безопасности	Александр Морковчин	2	2	11
7	Основные положения и методы защиты организации	Александр Морковчин	2	2	11

*ЗЕ - зачётная единица (1 ЗЕ=38 ак.часов) **1 академ.час = 40 мин.

Логика прохождения курса

Программа дисциплины состоит из 2 модулей, в которые включены 13 тем

Сроки реализации:

1 модуль: октябрь

2 модуль: ноябрь–декабрь

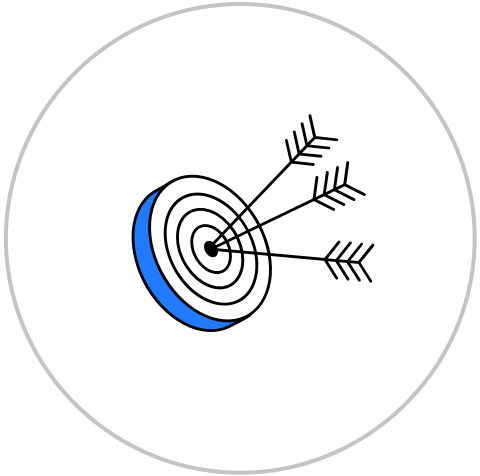
Содержание модулей:

1. Видеолекции (самостоятельное изучение)
2. Вебинары
3. Домашние задания (тесты или практические задания)

Записи вебинаров и презентации можно будет посмотреть на следующий день после пройденного занятия в группе

Цель дисциплины

Освоение компетенций, необходимых для осуществления профессиональной деятельности в сфере нормативного обеспечения кибербезопасности

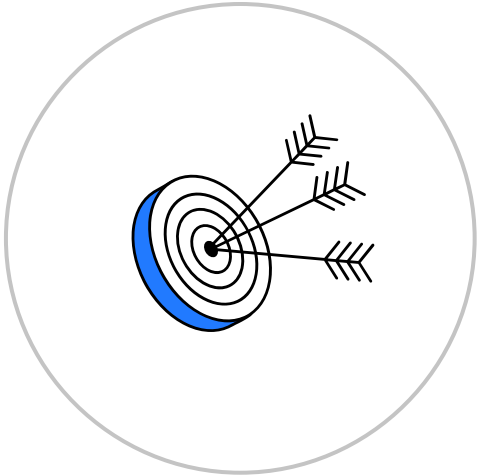


Планируемые результаты обучения. 1 модуль

Знать: цели, структуру и принципы нормативного обеспечения кибербезопасности

Уметь: обсуждать и аргументированно защищать свою точку зрения по правовым вопросам защиты информации

Владеть: навыками применения нормативно-правовой документации в профессиональной деятельности

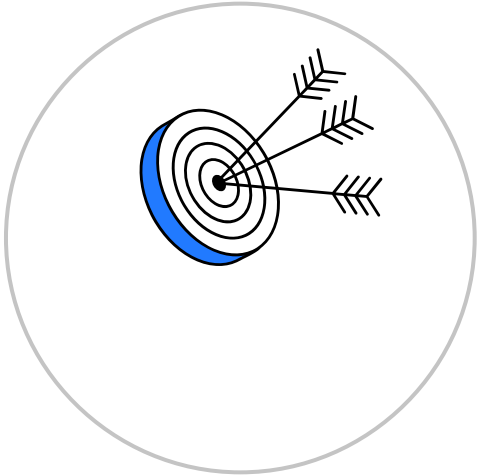


Планируемые результаты обучения. 2 модуль

Знать: область применения, структуру, принципы и необходимые процедуры в рамках международных и отраслевых стандартов в области информационной безопасности (ИБ) и лучшие практики обеспечения и управления ИБ

Уметь: обсуждать и аргументированно защищать свою точку зрения по вопросам применения стандартов и лучших практик обеспечения и управления ИБ

Владеть: навыками применения знаний о международных и отраслевых стандартах и лучших практик обеспечения и управления ИБ в профессиональной деятельности



1 тема. Введение в кибербезопасность

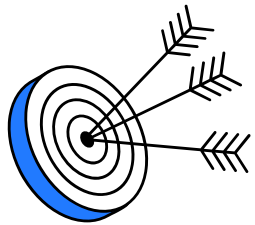
Формат учебного контента:

- видеолекция
- вебинар
- ДЗ (тест)

Знает и понимает пути возникновения и становления отрасли информационной безопасности в современном мире.

Умеет обобщать и классифицировать основные задачи информационной безопасности на территории РФ – как частные, так и глобальные.

Знает и понимает угрозы ИБ, их источники, основные методы противодействия им



Тема 2. Нормативное регулирование информационной безопасности

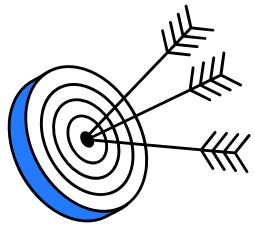
Формат учебного контента:

- видеолекция
- вебинар
- ДЗ (задание с самопроверкой)

Знает и понимает структуру информационных правоотношений, нормативно-правовые акты, регулирующие отрасль ИБ

Умеет проводить структурный анализ отраслевых документов

Применяет основные документы, регулирующие отрасль ИБ, в профессиональной деятельности



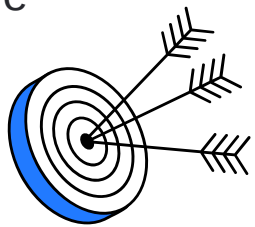
Тема 3. Режимы информации ограниченного доступа

Формат учебного контента:

- видеолекция
- вебинар
- ДЗ (задание с самопроверкой)

Знает и понимает основные документы по нормативному регулированию информации ограниченного доступа

Умеет применять НПА регулирующие сферу информации ограниченного доступа в профессиональной деятельности, в том числе в разработке технических заданий и создания сайтов



Тема 4. Классификация и категорирование информации, информационных систем

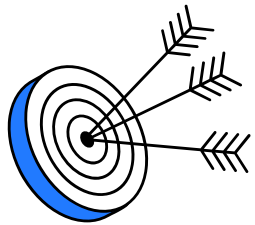
Формат учебного контента:

- видеолекция
- вебинар
- ДЗ (тест)

Классифицирует и категоризирует информационные системы для обеспечения ИБ

Умеет определять значение информационных систем для обеспечения ИБ

Владеет навыком категорирования объектов критической информационной инфраструктуры



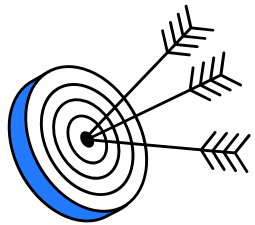
Тема 5. Лицензирование и сертификация

Формат учебного контента:

- видеолекция
- вебинар
- ДЗ (2 теста)

Знает и понимает основные документы по нормативному регулированию лицензирования, сертификации (подтверждения соответствия) и аккредитации в сфере информационных технологий

Умеет применять НПА по лицензированию и сертификации (подтверждению соответствия) и аккредитации в профессиональной деятельности.

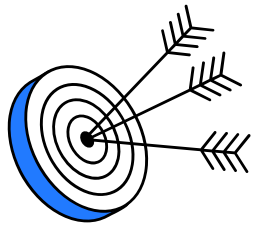


Тема 6. Правонарушения в сфере компьютерной информации

Формат учебного контента:

- видеолекция
- вебинар
- кейс игра
- ДЗ (проверяемое задание, тест)

Знает и понимает какие виды правонарушений в сфере компьютерной информации бывают и какая предусмотрена ответственность за них



Тема 7. Международные и отраслевые стандарты. GDPR

Формат учебного контента:

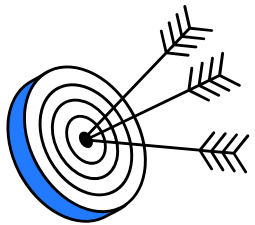
- вебинар
- ДЗ (тест)

Знает какие есть роли в GDPR и какие требования необходимо выполнять для соответствия европейскому регламенту

Понимает основные требования по защите данных по GDPR, DPIA

Знает в каких случаях и как уведомлять надзорные органы государств-членов Евросоюза об инциденте безопасности персональных данных, а также как накладываются штрафы в Европе по GDPR

Умеет определять, в каких случаях GDPR применим для российского и международного бизнеса



Тема 8. Международные и отраслевые стандарты. ISO 27001

Формат учебного контента:

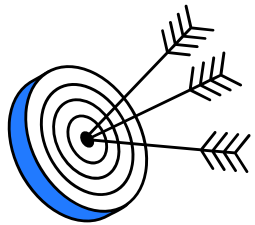
- видеолекция
- вебинар
- ДЗ (задание с самопроверкой)

Умеет ориентироваться в стандарте ISO 27001

Знает структуру стандарта ISO 27001

Знает как провести подготовку к международной сертификации СОИБ по стандарту ISO 27001

Имеет представление о процессе выполнения контролей из Приложения А



Тема 9. Международные и отраслевые стандарты. PCI DSS

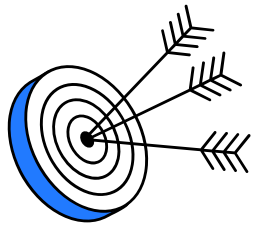
Формат учебного контента:

- видеолекция
- вебинар
- ДЗ (тест)

Умеет ориентироваться в стандарте PCI DSS

Знает процедуры прохождения сертификационного аудита

Умеет корректно определять область действия стандарта PCI DSS и заполнять отчет об оценке соответствия требованиям Стандарта



Тема 10. Международные и отраслевые стандарты. ISO 22301

Формат учебного контента:

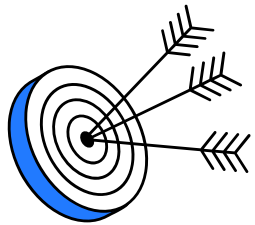
- видеолекция
- вебинар
- ДЗ (тест)

Знает стандарт ISO 22301, умеет ориентироваться в стандарте, объяснить назначение и содержание

Знает основные задачи и принципы УНБ

Знает основные элементы и действия в рамках цикла УНБ

Умеет объяснить почему BCM это важно и как может помощь организации



Тема 11. Управление рисками

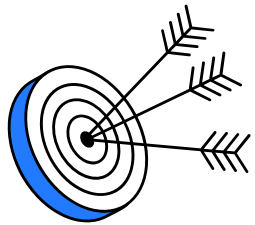
Формат учебного контента:

- видеолекция
- вебинар
- ДЗ (задание с проверкой)

Знает значение оценки рисков ИБ в профессиональной деятельности

Знает стандарты оценки рисков ИБ

Имеет навык в оценке рисков



Тема 12. Организация безопасности внутри компании. Ключевые аспекты построения системы безопасности

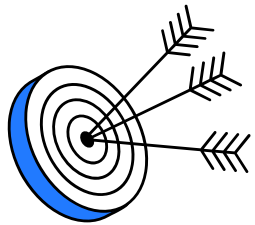
Формат учебного контента:

- видеолекция
- вебинар
- ДЗ (тест)

Знает функции информационной безопасности в корпоративной структуре компании

Знает обобщенный алгоритм формирования системы защиты смоделированного предприятия

Может сформировать системы защиты информации в организации



Тема 13. Основные положения и методы защиты организации

Формат учебного контента:

- видеолекция
- вебинар
- ДЗ (тест)

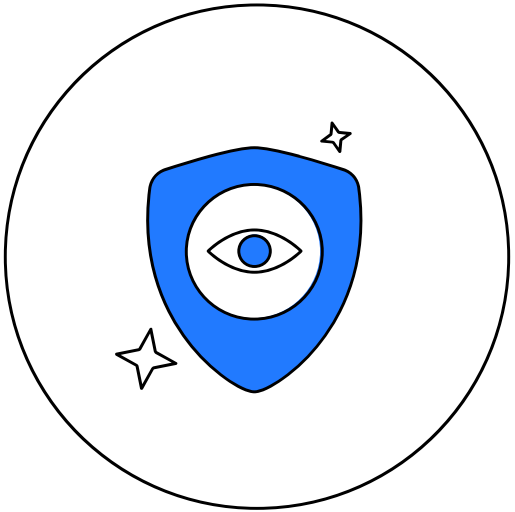
Знает ключевые шаги построения системы защиты

Знает особенности:

- внедрения отдельных процессов ИБ
- организации документационного обеспечения процессов ИБ
- организации технических мер обеспечения ИБ
- повышения осведомленности работников и выстраивания культуры ИБ
- построения системы контроля и измерения ИБ

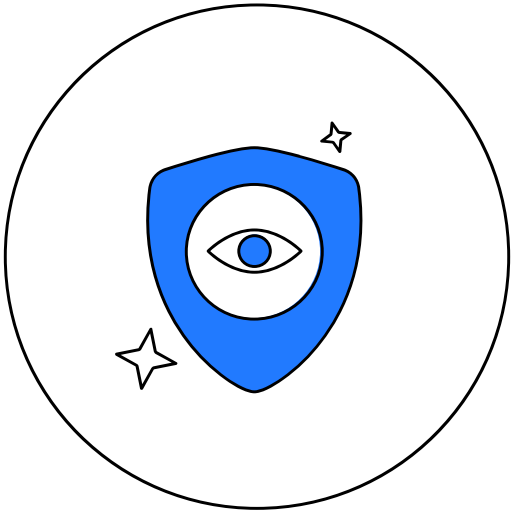
Практика в модуле 1

- Разработка инструкции для пользователя по соблюдению правил информационной безопасности на рабочем месте
- Анализ документа (Согласия на обработку персональных данных) на предмет соблюдения требований законодательства
- Групповая кейс-игра (суд за правонарушение в области компьютерной информации)



Практика в модуле 2

- Описание реализации группы контролей по ISO 27002 (стандарт информационной безопасности, опубликованный организациями ISO и IEC)
- Оценка рисков (способы оценки рисков, идентификация рисков, анализ рисков, оценивание рисков) по международным и отраслевым стандартам (ISO 31000, ISO 27005, NIST SP 800, 716-П)



Оценивание по дисциплине

1. Промежуточная аттестация по дисциплине включает в себя:
   - 4 домашних задания проверяемых преподавателем (темы 6, 7, 8)
   - 2 домашних задания с самопроверкой по чек-листу (темы 2, 3, 11)
   - 10 домашних работ в форме теста по остальным темам дисциплины
   - участие групповой кейс-игре (тема 6)
2. Итоговая аттестация по дисциплине — **экзамен** в **форме итогового теста**

Оценивание по дисциплине

3 Итоговая оценка за дисциплину формируется как взвешенная сумма оценок за отдельные элементы контроля и оценки за экзамен

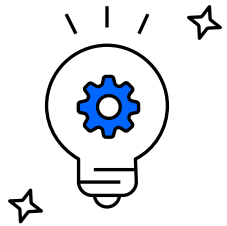
№	Элемент контроля	Весовой коэффициент
1	Экзамен (итоговое тестирование)	0.3
2	Домашние задания с проверкой	0.4
3	Тесты и домашние задания с самопроверкой	0.2
4	Кейс-игра	0.1

Важно

1. Дедлайн сдачи домашнего задания:
   - тест — 3 рабочих дня после окончания вебинара
   - задание — 6 рабочих дней после окончания вебинара

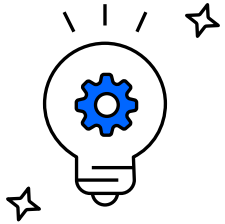
2. Тест считается зачтённым если дано 80% правильных ответов и выше

3. Задание (в рамках ДЗ) считается зачтённым, если выполнены все пункты чек-листа



Шкала соответствия оценок в НИУ ВШЭ

Оценка по 10-ти бальной шкале	Оценка по 5-ти бальной шкале за экзамен	Оценка в приложении к диплому НИЯУ ВШЭ	
10	отлично (существенно превосходит ожидания)	A ++	Excellent
9	отлично (превосходит ожидания)	A +	Very good
8	отлично	A	Very good
7	хорошо	B +	Good
6	хорошо	B -	Good
5	удовлетворительно	C +	Satisfactory
4	удовлетворительно	C -	Satisfactory
3	неудовлетворительно	F	Fail
2	неудовлетворительно	F	Fail
1	неудовлетворительно	F	Fail



Вы узнали

1. Преподавателей-экспертов дисциплины
2. В какой последовательности изучать дисциплину
3. Какими знаниями, умениями и навыками вы будете обладать
4. Как получить аттестацию по дисциплине

Нормативное обеспечение кибербезопасности

Оксана Докучаева
Академический руководитель дисциплины