Описание Учебного Курса

Название	Жизненный цикл, принципы и передовой опыт разработки и реализации национальной стратегии кибербезопасности
Модальность	Электронное обучение и виртуальные классы (eLearning and virtual class)
Сроки	Не определены
Продолжительность	4 часа электронного обучения 2 часа виртуального класса (только для национальных/региональных групп, по отдельному запросу)
Предельный срок регистрации	Не определен
Плата за обучение	Бесплатно

Описание	Кибербезопасность – это комплексная проблема, которая включает несколько различных управленческих, политических, эксплуатационных, технических и правовых аспектов. Этот онлайновый курс позволяет получить общие знания, которые помогут рассмотреть, упорядочить и выстроить в приоритетном порядке многие из этих областей на основе существующих, широко признанных моделей, систем и других справочных материалов. В ходе обучения особое внимание уделяется элементам защиты гражданских аспектов киберпространства и поэтому рассматриваются общие принципы и примеры передового опыта, которые необходимо учитывать в процессе подготовки проекта, разработки национальной стратегии кибербезопасности и управления ею. Для этого в ходе обучения проводится четкое различие между "процессом", который будет принят странами во время жизненного цикла национальной стратегии кибербезопасности (инициирование, критический обзор и анализ, создание, реализация, мониторинг и оценка), и "содержанием", то есть фактическим текстом, который появится в документе о национальной стратегии кибербезопасности. Этот курс обучения не охватывает такие аспекты, как развитие наступательных или оборонительных киребвозможностей военными структурами, силами обороны или разведывательными службами страны. В ходе обучения будет предоставлен также обзор базовых компонентов, необходимых странам для того, чтобы они могли стать киберподготовленными, будут выделены важные аспекты, которые правительства должны учитывать при разработке своих национальных стратегий и планов реализации. И, наконец, во время этого обучения представителям директивных органов будет предоставлен всеобъемлющий общий обзор существующих подходов и приложений со ссылкой на дополнительные источники, которые могут быть использованы при реализации конкретных видов деятельности в области кибербезопасности на национальном уровне.
Код курса	22OS500033CIS-R-D

1. ЦЕЛИ УЧЕБНОГО КУРСА

Цель данного учебного курса состоит в том, чтобы выработать у руководителей и представителей директивных органов стратегическое мышление в вопросах кибербезопасности на национальном уровне. После прохождения этого обучения пользователи смогут достичь следующих результатов:

- Ознакомятся с основными понятиями и определениями кибербезопасности и получат прочные базовые знания о том, как кибербезопасность функционирует на национальном уровне.

- Ознакомятся с руководством по разработке национальной стратегии кибербезопасности.
- Усвоят пять этапов жизненного цикла национальной стратегии кибербезопасности (инициирование; критический обзор и анализ; создание; реализация; мониторинг и оценка)
- Усвоят основополагающие принципы, которые должны учитываться при разработке перспективной и всеобъемлющей национальной стратегии кибербезопасности.
- Ознакомятся с соответствующим передовым опытом в области кибербезопасности, а с также тем, как его можно применить в национальном контексте.

2. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

В конце учебного курса пользователи смогут:

- усвоить основные понятия и определения кибербезопасности, а также понять, как кибербезопасность функционирует на национальном уровне;
- эффективно использовать руководство по разработке национальной стратегии кибербезопасности;
- понять пять этапов жизненного цикла национальной стратегии кибербезопасности (инициирование, критический обзор и анализ, создание, реализация, мониторинг и оценка) и как они могут быть реализованы в национальном контексте;
- понять основополагающие принципы, которые должны учитываться при разработке перспективной и всеобъемлющей национальной стратегии кибербезопасности;
- понять соответствующий передовой опыт в области кибербезопасности и как его можно применить в национальном контексте.

3. ЦЕЛЕВАЯ АУДИТОРИЯ

Этот курс национальной стратегии кибербезопасности предназначен в первую очередь для представителей директивных органов, ответственных за разработку национальной стратегии кибербезопасности. Вторичной аудиторией являются все остальные заинтересованные стороны из государственного и частного секторов, участвующие в разработке и реализации стратегии, например ответственные сотрудники государственных органов, сотрудники регуляторных органов, органов правопорядка, поставщики услуг ИКТ, операторы критических инфраструктур, представители гражданского общества, академических организаций и научно-исследовательских учреждений. Обучение может также оказаться полезным для различных заинтересованных сторон в международном сообществе в сфере развития, которые оказывают помощь в области кибербезопасности.

4. ТРЕБОВАНИЯ К УЧАСТНИКАМ

Участники должны быть приглашены для прохождения курса.

Чтобы участвовать в этом курсе, никаких специальных квалификаций или опыта не требуется. Пользователям предлагается запросить это обучение на платформе

Академии МСЭ. Группа МСЭ по кибербезопасности рассмотрит соответствующие запросы и подтвердит участие. Приоритет отдается представителям директивных органов, ответственным за разработку национальной стратегии кибербезопасности.

5. СОДЕРЖАНИЕ УЧЕБНОГО КУРСА

Обучение построено на базе четырех модулей электронного обучения и одних онлайновых настольных учений, которые основаны на Руководстве по разработке национальной стратегии кибербезопасности. Содержание обучения будет охватывать следующие темы:

- Модуль 0 (Введение): знакомит участников с основными понятиями и определениями кибербезопасности и обеспечивает прочные базовые знания о том, как кибербезопасность функционирует на национальном уровне.
- Модуль 1: содержит обзор различных этапов разработки стратегии, которые включают:
  - инициирование
  - критический обзор и анализ
  - создание национальной стратегии кибербезопасности
  - реализация
  - мониторинг и оценка
- Модуль 2: содержит основополагающие принципы, которые помогают в разработке перспективной и всеобъемлющей национальной стратегии кибербезопасности, а именно:
  - видение национальной стратегии кибербезопасности
  - комплексный подход
  - открытость
  - социально-экономическое благополучие
  - основные права человека
  - управление рисками и способность к восстановлению
  - инструменты политики
  - руководство, распределение функций и ресурсов
  - доверительная среда
- Модуль 3: представляет набор элементов передового опыта, которые делают стратегию всеобъемлющей и эффективной и в то же время позволяют адаптировать ее к национальному контексту. Эти элементы передового опыта сгруппированы по следующим областям деятельности:
  - управление
  - управление рисками в области национальной кибербезопасности
  - подготовленность и способность к восстановлению
  - услуги критических инфраструктур и важнейшие услуги
  - возможности и создание потенциала, а также повышение осведомленности
  - законодательство и регулирование
  - международное сотрудничество
- Настольные учения (организуются для национальных/региональных групп по запросу): виртуальные настольные учения – это сессии, во время которых пользователи встречаются в виртуальном классе и имеют возможность обсудить приобретенные знания путем постановки практических заданий и направленного обсуждения. Эти настольные учения будут посвящены содержанию обучения и практическому опыту, а также передовому опыту, которым участники хотели бы поделиться.

6. ГРАФИК УЧЕБНОГО КУРСА

Сессия	Тема	Упражнения и взаимодействие
Начальный тест	Основы кибербезопасности	Обучение со свободным графиком. Если проходной бал набран (24 правильных ответа из 30), пользователи перенаправляются в модуль 1. Если проходной бал не набран, пользователи должны будут пройти модуль 0 и соответствующий тест
Модуль 0 + тест	Основы кибербезопасности	Обучение со свободным графиком (1 час). Посещение этого модуля и успешное прохождение теста обязательны для того, чтобы перейти к следующему заданию. Если тест пройден не удачно, пользователь должен будет повторно пройти этот модуль и тест
Модуль 1 + тест	Жизненный цикл национальной стратегии кибербезопасности	Обучение со свободным графиком (1 час). Посещение этого модуля и успешное прохождение теста обязательны для того, чтобы перейти к следующему заданию. Если тест пройден не удачно, пользователь должен будет повторно пройти этот модуль и тест
Модуль 2 + тест	Принципы национальной стратегии кибербезопасности	Обучение со свободным графиком (1 час). Посещение этого модуля и успешное прохождение теста обязательны для того, чтобы перейти к следующему заданию. Если тест пройден не удачно, пользователь должен будет повторно пройти этот модуль и тест
Модуль 3 + тест	Передовой опыт национальной стратегии кибербезопасности	Обучение со свободным графиком (1 час). Посещение этого модуля и успешное прохождение теста обязательны для того, чтобы перейти к следующему заданию и получения свидетельства о прохождении. Если тест пройден не удачно, пользователь должен будет повторно пройти этот модуль и тест
Практическое задание	Жизненный цикл, принципы и передовой опыт национальной стратегии кибербезопасности	Обучение со свободным графиком (офлайн) организуются для национальных/региональных групп по запросу. При регистрации для настольных учений пользователи получат практическое задание. Пользователи должны представить выполненное задание не позднее, чем за 5 дней до настольных учений. Своевременное представление является обязательным условием участия в настольных учениях.
Виртуальные настольные учения	Жизненный цикл, принципы и передовой опыт национальной стратегии кибербезопасности	Виртуальный класс (2 часа). После прохождения модулей электронного обучения у пользователей будет один год, чтобы зарегистрироваться для виртуальных настольных учений. МСЭ организует регулярные сессии настольных учений, и пользователи могут выбрать удобную для них дату. Посещение настольных учений является обязательным для завершения обучения и получения свидетельства о прохождении курса обучения

7. МЕТОДИКА (Дидактический подход)

Обучение будет проводиться полностью в онлайновом режиме и будет сочетать в себе различные дидактические подходы:

- **4 модуля электронного обучения со свободным графиком**: Модули 0, 1, 2 и 3 – это цифровые курсы обучения со свободным графиком проведения, представленные в виде слайдов с информацией и носителями информации (видео, аудио и изображения). Эти модули содержат элементы игрофикации, в частности, вопросники, моделирование, перетаскивания объектов мышью и т. д. Это модули обучения со свободным графиком прохождения, что позволяет пользователям самостоятельно организовать свой процесс познания и пройти эти модули.
- **4 цифровых теста**: Каждый из этих модулей предусматривает цифровой тест, включающий до 30 вопросов, чтобы проверить знания и успехи в обучении, достигнутые пользователями. Эти тесты включают различного рода вопросы (например, вопросы да/нет, вопросы с несколькими вариантами ответа, ответвление, перетаскивание объектов мышью и т. д.).
- **1 практическое задание**: После прохождения модулей электронного обучения участникам, вовлечённым в прохождение практические занятия, будет дано практическое задание, которое они должны будут выполнить самостоятельно офлайн. Обычно это задание включает ряд теоретических и практических вопросов, охватывающих жизненный цикл, принципы и главные области деятельности в сфере национальной стратегии кибербезопасности. При этом нет правильных и неправильных ответов на эти вопросы, однако они рассчитаны на: a) усиление стратегического планирования; b) выработку критического мышления; c) повышение осведомленности о национальном контексте кибербезопасности; d) стимулирование решения проблем; e) совместное использование извлеченных уроков. Участники должны будут вернуть выполненные задания не позднее, чем за 5 дней до онлайнового обсуждения.
- **1 настольное учение**: Практические занятия и настольные учения организуются для национальных/региональных групп по запросу Виртуальные настольные учения – это сессии, где пользователи встречаются в виртуальном классе и имеют возможность обсудитьприобретенные знания путем направленного диалога в рамках группы пленарного заседания. Чтобы добиться максимальной отдачи от процесса образования, руководить настольными учениями будут координаторы из МСЭ, которые будут следить за ходом обучения. Координаторы будут также стимулировать обсуждение и выделять в ходе него соответствующие темы, проблемы, извлеченные уроки, решения и области, требующие улучшения. Онлайновые обсуждения будут включать элементы взаимодействия и игрофикации (голосования, интерактивные панели и т. д.). Настольные учения будут проводиться в онлайновом режиме на базе платформы в Zoom.

8. ОЦЕНКА И ПРОСТАВЛЕНИЕ ОЦЕНОК

Чтобы успешно завершить обучение и получить свидетельство о прохождении курса обучения, все участники должны будут пройти следующие элементы:

- Начальный тест: Обучение начинается с начального теста, включающего до 30 вопросов, чтобы оценить знания участников и понимание ими вопросов кибербезопасности и национальной стратегии кибербезопасности. Если проходной бал (80% правильных ответов) набран, соответствующий участник

перенаправляются в модуль 1. И, напротив, если проходной бал не набран, участники должны будут посетить модуль 0 и успешно пройти повторный тест.

- Тесты по прохождении всех модулей: Прохождение всех модулей завершается оценочным тестом, включающим до 30 вопросов, чтобы оценить успехи в обучении, достигнутые пользователями. Успешное прохождение теста (не менее 60% правильных ответов) необходимо для перехода к следующему модулю. Если этот тест пройден не удачно, пользователи должны будут повторно пройти этот модуль и, соответственно, этот тест.
- Практическое задание: Участники должны будут вернуть выполненные задания не позднее, чем за 5 дней до виртуальных настольных учений. Это задание не оценивается, однако его выполнение и своевременное представление необходимо для участия в настольных учениях.
- Виртуальные настольные учения: Посещение виртуальных настольных учений обязательно для завершения прохождения обучения. Хотя на этом этапе обучения оценка не проставляется, ожидается, что участники примут активное участие в обсуждении и деятельности, проводимой во время этого учения (игрофикация, голосования, интерактивные панели и т. д.).

9. КООРДИНАЦИЯ УЧЕБНОГО КУРСА

Координатор курса:	**Координатор МСЭ**:
Фамилия:	Фамилия: Фарид Нахли (Farid Nakhli)
Адрес электронной почты:	Адрес электронной почты: farid.nakhli@itu.int