[](https://crossmark.crossref.org/dialog/?doi=10.6028/NIST.SP.800-50r1)**Создание системы кибербезопасности и конфиденциальности**

**Программа обучения**

Мэриан Мерритт Сьюзан Ханше Доктор Бренда Эллис

Кевин Санчес-Черри Джули Нетери Снайдер Дональд Уолден

Данная публикация доступна бесплатно по адресу: https://doi.org/10.6028/NIST.SP.800-50r1



**Создание системы кибербезопасности и конфиденциальности**

**Программа обучения**

Мариан Мерритт, *подразделение прикладной кибербезопасности, лаборатория информационных технологий*

Сьюзан Ханше

*Кибербезопасность и инфраструктура*

*Агентство безопасности Министерство внутренней безопасности*

Доктор Бренда Эллис

*Национальная федерация аэронавтики и космонавтики*

*Администрация*

Кевин Санчес-Черри *Офис директора по информационным технологиям Департамента транспорта*

Джули Нетери Снайдер

*МИТРА*

Дональд Уолден

*Налоговое управление США*

Данная публикация доступна бесплатно по адресу: https://doi.org/10.6028/NIST.SP.800-50r1

Сентябрь 2024



Министерство торговли США

*Джина М. Раймондо, секретарь*

Национальный институт стандартов и технологий

*Лори Э. Локасцио, директор NIST и заместитель министра торговли по стандартам и технологиям*

Определенное оборудование, инструменты, программное обеспечение или материалы, коммерческие или некоммерческие, указаны в этом документе для адекватного определения экспериментальной процедуры. Такая идентификация не подразумевает рекомендацию или одобрение какого-либо продукта или услуги со стороны NIST, а также не означает, что указанные материалы или оборудование обязательно являются наилучшими доступными для этой цели.

В данной публикации могут содержаться ссылки на другие публикации, которые в настоящее время разрабатываются NIST в соответствии с возложенными на него уставными обязанностями. Информация, содержащаяся в данной публикации, включая концепции и методологии, может быть использована федеральными агентствами еще до завершения подготовки таких сопутствующих публикаций.

Таким образом, до тех пор, пока каждая публикация не будет завершена, текущие требования, руководящие принципы и процедуры, если они существуют, остаются в силе. В целях планирования и перехода федеральные агентства, возможно, пожелают внимательно следить за разработкой этих новых публикаций NIST.

Организациям рекомендуется просматривать все проекты публикаций во время периодов общественного обсуждения и предоставлять отзывы в NIST. Многие публикации NIST по кибербезопасности, кроме отмеченных выше, доступны по адресу [https://csrc.nist.gov/publications.](https://csrc.nist.gov/publications)

**Авторитет**

Данная публикация была разработана NIST в соответствии с его уставными обязанностями в соответствии с Федеральным законом о модернизации информационной безопасности (FISMA) от 2014 года, 44 U.S.C. § 3551 и далее, Публичное право (P.L.) 113-283. NIST отвечает за разработку стандартов и руководящих принципов информационной безопасности, включая минимальные требования к федеральным информационным системам, но такие стандарты и руководящие принципы не должны применяться к системам национальной безопасности без специального одобрения соответствующих федеральных должностных лиц, осуществляющих политические полномочия в отношении таких систем. Это руководство соответствует требованиям циркуляра A-130 Административно-бюджетного управления (OMB).

Ничто в этой публикации не должно противоречить стандартам и руководящим принципам, которые стали обязательными и обязательными для федеральных агентств министром торговли в соответствии с законодательными полномочиями. Кроме того, эти руководящие принципы не должны толковаться как изменяющие или заменяющие существующие полномочия министра торговли, директора OMB или любого другого федерального должностного лица. Данная публикация может использоваться неправительственными организациями на добровольной основе и не является объектом авторского права в Соединенных Штатах. Тем не менее, NIST высоко оценил бы атрибуцию.

**Политика NIST в отношении технических серий**

[Заявления об авторских правах, использовании и лицензировании](https://doi.org/10.6028/NIST-TECHPUBS.CROSSMARK-POLICY)

[Синтаксис идентификатора публикации технической серии NIST](https://www.nist.gov/document/publication-identifier-syntax-nist-technical-series-publications)

**История публикаций**

Одобрено редакционным советом NIST 2024-08-09

Заменяет NIST SP 800-50 (октябрь 2003) [https://doi.org/10.6028/NIST.SP.800-50;](https://doi.org/10.6028/NIST.SP.800-50) Заменяет NIST SP 800-16 (апрель 1998) <https://doi.org/10.6028/NIST.SP.800-16>

**Как цитировать эту публикацию технической серии NIST:**

Мерритт М., Ханше С., Эллис Б., Санчес-Черри К., Снайдер Дж.Н., Уолден Д. (2024) Создание программы обучения кибербезопасности и конфиденциальности. (Нати[Национальный институт стандартов и технологий](https://doi.org/10.6028/NIST.SP.800-50r1), Гейтерсбург, штат Мэриленд), специальное издание NIST (SP) NIST SP 800-50r1. https://doi.org/10.6028/NIST.SP.800-50r1

**Автор ORCID iDs**

Мэриан Мерритт: 0000-0002-2116-8959

**Контактная информация**

[sp800-50-comments@nist.gov](mailto:sp800-50-comments@nist.gov)

Национальный институт стандартов и технологий

Кому: Отдел прикладной кибербезопасности, Лаборатория информационных технологий 100 Bureau Drive (Mail Stop 2000) Гейтерсберг, Мэриленд 20899-2000

**Дополнительная информация**

Дополнительная информация об этой публикации доступна по адресу [https://csrc.nist.gov/pubs/sp/800/50/r1/final,](https://csrc.nist.gov/pubs/sp/800/50/r1/final) включая соответствующий контент, потенциальные обновления и историю документов.

**Все комментарии подлежат публикации в соответствии с Законом о свободе информации (FOIA).**

# Абстрактный

В этой публикации содержатся рекомендации для федеральных агентств и организаций по разработке и управлению подходом к созданию Программы обучения кибербезопасности и конфиденциальности (CPLP) на основе жизненного цикла. Этот подход предназначен для удовлетворения потребностей больших и малых организаций, а также тех, кто создает совершенно новую программу. Информация основана на широко принятых стандартах, правилах, законодательстве и передовых практиках. Рекомендации являются настраиваемыми и могут быть реализованы в рамках общеорганизационного процесса, который управляет информационными, учебными и образовательными программами для различных аудиторий федеральных служащих. Программа должна поощрять изменение поведения в рамках управления рисками и привести к развитию культуры конфиденциальности и безопасности в организации. Руководство также включает в себя предлагаемые показатели и методы оценки для регулярного улучшения и обновления программы по мере развития потребностей.

# Ключевые слова

осознание; изменение поведения; кибербезопасность; образование; программа обучения; конфиденциальность; культура неприкосновенности частной жизни; ролевые; культура безопасности; тренировка.

# Доклады по технологиям компьютерных систем

Лаборатория информационных технологий (ITL) Национального института стандартов и технологий (NIST) содействует развитию экономики США и общественному благосостоянию, обеспечивая техническое лидерство для национальной инфраструктуры измерений и стандартов. ITL разрабатывает тесты, методы испытаний, справочные данные, экспериментальные реализации концепций и технические анализы для продвижения развития и продуктивного использования информационных технологий. В обязанности ITL входит разработка управленческих, административных, технических и физических стандартов и руководящих принципов для экономически эффективной кибербезопасности и конфиденциальности информации, не связанной с национальной безопасностью, в федеральных информационных системах. В Специальном издании серии 800 сообщается об исследованиях, руководящих принципах и информационно-разъяснительной работе ITL в области безопасности информационных систем, а также о ее совместной деятельности с промышленностью, государственными и академическими организациями.

# Уведомление о раскрытии патентной информации

ПРИМЕЧАНИЕ: ITL обратилась к держателям патентных притязаний, использование которых может потребоваться для соблюдения руководящих указаний или требований настоящей публикации, сообщить ITL о таких патентных притязаниях. Тем не менее, владельцы патентов не обязаны отвечать на запросы ITL о выдаче патентов, и ITL не проводила патентный поиск с целью определить, какие патенты, если таковые имеются, могут применяться к данной публикации.

На дату публикации и после запроса (запросов) для выявления патентных притязаний, использование которых может потребоваться для соблюдения руководящих указаний или требований настоящей публикации, в ITL не было выявлено ни одной такой патентной формулы изобретения.

ITL не делает никаких заявлений и не подразумевает, что лицензии не требуются для предотвращения нарушения патентных прав при использовании данной публикации.

# Содержание

[**Резюме 1**](#_bookmark0)

1. [**Знакомство 3**](#_bookmark4)



* + 1. [Основные понятия управления рисками конфиденциальности 9](#_bookmark14)
    2. [Координация усилий по обучению кибербезопасности и конфиденциальности 10](#_bookmark17)
    3. [Руководитель организационного отдела 11](#_bookmark20)
    4. [Высшее руководство 12](#_bookmark22)
    5. [Менеджеры CPLP 12](#_bookmark23)
    6. [Менеджеры 13](#_bookmark24)
    7. [Пользователь системы 14](#_bookmark25)

1. [План и стратегия CPLP 15](#_bookmark26)
   * 1. [Примеры заявлений о политике программы обучения 17](#_bookmark29)
     2. [Сценарий 1: Защита конфиденциальных печатных данных 19](#_bookmark33)
     3. [Сценарий 2: Разработка новой программы обучения, соответствующей нормативным требованиям 20](#_bookmark34)
     4. [Измерения 21](#_bookmark36)
     5. [От измерений к метрикам 24](#_bookmark38)
     6. [Все пользователи 26](#_bookmark41)
     7. [Владельцы учетных записей с привилегированным доступом 27](#_bookmark43)
     8. [Сотрудники, выполняющие значительные обязанности в области кибербезопасности и/или неприкосновенности частной жизни 28](#_bookmark44)
     9. [Определение того, кто несет значительную ответственность за кибербезопасность и/или неприкосновенность частной жизни 28](#_bookmark45)
     10. [Упражнения по повышению осведомленности 30](#_bookmark48)
     11. [Эмпирическое обучение 30](#_bookmark49)
     12. [Содержание тренинга 31](#_bookmark50)



* + 1. [Определение бюджета СПЯС 33](#_bookmark55)
    2. [Персонал и местонахождение CPLP 35](#_bookmark56)

1. [**Анализ и проектирование CPLP 38**](#_bookmark58)
   * 1. [Важность этапа анализа 39](#_bookmark61)
     2. [Этапы этапа анализа 40](#_bookmark62)
     3. [Этапы этапа проектирования 43](#_bookmark65)
2. [**Разработка и внедрение СПЯС 49**](#_bookmark72)
   * 1. [Общие руководящие принципы разработки или приобретения новых материалов CPLP 49](#_bookmark74)
     2. [Разработка новых материалов для программы обучения «Все пользователи» 51](#_bookmark76)
     3. [Разработка новых материалов для Программы обучения владельцев учетных записей с привилегированным доступом 52](#_bookmark78)
     4. [Разработка новых материалов для тех, кто обладает высоким уровнем кибербезопасности и/или конфиденциальности](#_bookmark79) [Обязанности 53](#_bookmark79)
     5. [Получение учебных материалов из внешних источников 53](#_bookmark80)
     6. [Проведение тестирования учащихся на новых элементах CPLP 53](#_bookmark81)
     7. [Шаги по реализации нового элемента CPLP 54](#_bookmark83)



1. [**Оценка и совершенствование CPLP 57**](#_bookmark89)
   * 1. [Измерения и метрики 58](#_bookmark92)
     2. [Отчетность о соответствии нормативным требованиям 58](#_bookmark93)
     3. [Оценка эффективности CPLP 59](#_bookmark94)

[5.2.4. Рассмотрение Отчета об оценке CPLP с высшим руководством 64](#_bookmark98)

1. [**Сводка 66**](#_bookmark100)

[**Ссылки 67**](#_bookmark101)

[**Приложение А. Примеры уровней зрелости программы обучения по кибербезопасности и конфиденциальности 69**](#_bookmark119)

[**Приложение Б. Глоссарий 72**](#_bookmark121)

[**Приложение В. Журнал изменений 77**](#_bookmark122)

# Список столов

[**Таблица 1. Элементы стратегии CPLP 19**](#_bookmark32)

[**Таблица 2. Примеры целей, задач и результатов обучения 22**](#_bookmark37)

[**Таблица 3. Примеры уровней зрелости CPLP 69**](#_bookmark120)

# Список рисунков

[**Рис 1. Жизненный цикл программы обучения по кибербезопасности и конфиденциальности 6**](#_bookmark9)

[**Рис 2. Взаимосвязь между рисками кибербезопасности и конфиденциальности 8**](#_bookmark12)

[**Рис 3. Взаимосвязь между рисками неприкосновенности частной жизни и организационными рисками 10**](#_bookmark16)

[**Рис 4. Сегменты аудитории обучающей программы CPLP 26**](#_bookmark40)

**Подтверждения**

Это издание было разработано усилиями преданной команды авторов-добровольцев. Выражаем благодарность Джессике Диксон, Национальный институт стандартов и технологий (NIST); Сюзанна Фурман, NIST; Джули Хейни, NIST; Дэн Джейкобс, Управление по управлению персоналом; Джоди Джейкобс, NIST; Эрик Грей, Департамент образования; Сара Моффатт, Национальные институты здравоохранения; Дилан Гилберт, NIST; Наоми Лефковиц, NIST; Джереми Ликата, NIST; Родни Петерсен, NIST; Эдуардо Такамура, NIST; и Виктория Ян Пиллиттери, NIST.

# Резюме

Обеспечение того, чтобы сотрудники федеральной организации были осведомлены и готовы надлежащим образом и эффективно реагировать на риски кибербезопасности и конфиденциальности, является важной задачей, требующей стратегического подхода, основанного на продуманном планировании, соображениях ресурсов и принятии решений руководством. Это долгожданное обновление специальной публикации NIST 2003 года (SP) 800-50 « *Создание программы повышения осведомленности и обучения безопасности информационных технологий»* содержит рекомендации по созданию и управлению программой, которая включает в себя кампании по повышению осведомленности о кибербезопасности и конфиденциальности, ролевое обучение и другие программы обучения персонала. Эти программы объединяются в общую программу обучения кибербезопасности и конфиденциальности (CPLP), которая является частью более широких организационных усилий по снижению рисков кибербезопасности и конфиденциальности. Итоговый CPLP поддерживает федеральные требования и включает в себя признанные в отрасли передовые методы управления рисками.

В дополнение к выполнению установленных законом обязанностей в соответствии с Федеральным законом об управлении информационной безопасностью (FISMA) [ [2]](#_bookmark103), эта специальная публикация поддерживает Закон о полномочиях на национальную оборону от 2021 года (NDAA) [[1]](#_bookmark102) для «публикации стандартов и рекомендаций по повышению осведомленности сотрудников и подрядчиков федеральных агентств в области кибербезопасности».[1](#_bookmark1) Включение неприкосновенности частной жизни в качестве основополагающего элемента в CPLP отражает руководство, содержащееся в обновленном в 2016 году циркуляре A-130 Административно-бюджетного управления (OMB):

С. В нем также подчеркивается роль как конфиденциальности, так и безопасности в жизненном цикле федеральной информации. Важно отметить, что включение конфиденциальности представляет собой переход от рассмотрения требований безопасности и неприкосновенности частной жизни как простых мер по соблюдению требований к пониманию безопасности и неприкосновенности частной жизни как важнейших и взаимосвязанных элементов всеобъемлющей, стратегической и непрерывной программы, основанной на оценке рисков, в федеральных агентствах. [[3]](#_bookmark104)

Кроме того, это обновление включает элементы, ранее встречавшиеся в SP 800-16 «*Требования к обучению безопасности информационных технологий: модель на основе ролей и производительности*[» [4]](#_bookmark105), в котором определены рабочие роли федеральных агентств и организаций, требующие специализированного ролевого обучения задачам и навыкам кибербезопасности. Соответствующее содержание из SP 800-16 было включено в эту публикацию или было включено в SP 800-181r1 [[5].](#_bookmark106) В результате, SP 800-16 будет отозван после выхода данной публикации.

Каждый сотрудник организации играет свою роль в успехе эффективной программы кибербезопасности и конфиденциальности. Для тех, чьи должностные обязанности, связанные с информационными технологиями, кибербезопасностью или кибербезопасностью, требуют дополнительного или специального обучения, NICE Workforce Framework для

1 Раздел 9402 NDAA за 21 финансовый год «*Разработка стандартов и руководящих принципов для улучшения кадровой базы в области кибербезопасности федеральных агентств»* вносит поправки в Закон NIST следующим образом: «(b): ПУБЛИКАЦИЯ СТАНДАРТОВ И РУКОВОДЯЩИХ ПРИНЦИПОВ ПО ПОВЫШЕНИЮ ОСВЕДОМЛЕННОСТИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ. Не позднее чем через три года после даты вступления в силу настоящего Закона директор Национального института стандартов и технологий должен опубликовать стандарты и руководящие принципы для повышения осведомленности сотрудников и подрядчиков федеральных агентств в области кибербезопасности».

Кибербезопасность (NICE Framework)[2](#_bookmark2) [[5]](#_bookmark106) определяет конкретные знания и навыки, необходимые для выполнения задач, связанных с рабочими ролями в этих областях.[3](#_bookmark3)

Пользователи этой публикации найдут рекомендации о шагах, необходимых для:

* Создание эффективной CPLP для всего персонала федеральной организации, включая сотрудников и подрядчиков, что приведет к улучшению норм и поведения, снижающих риски кибербезопасности и конфиденциальности для организации при одновременном создании культуры конфиденциальности и безопасности
* Выявление персонала, нуждающегося в повышении квалификации
* Создание методологии оценки программы
* Участвуйте в постоянном улучшении программы

В каждом разделе содержатся рекомендации, позволяющие программе постоянно развиваться и совершенствоваться, тем самым сводя к минимуму риски для конфиденциальности и безопасности организации.

Настоящий документ определяет этапы управления CPLP и организован следующим образом:

* Раздел [1](#_bookmark4): Введение
* Раздел [2](#_bookmark26): [План и стратегия CPLP](#_bookmark26)
* Раздел [3](#_bookmark58): Анализ и дизайн [CPLP A](#_bookmark58)
* Раздел [4](#_bookmark72): Разработка и осуществление [CPLP](#_bookmark72)
* Раздел [5:](#_bookmark89) Оценка и совершенствование [CPLP A](#_bookmark89)

2 Национальная инициатива по образованию в области кибербезопасности (NICE) возглавляется NIST в Министерстве торговли США.

3 На момент подготовки данной публикации NIST возглавляет усилия по развитию персонала в области конфиденциальности, чтобы создать компаньона для NICE в области конфиденциальности.

# Знакомство

Снижение и управление рисками кибербезопасности и конфиденциальности требуют постоянного внимания со стороны всех сотрудников организации. Ключевым компонентом планов организации по кибербезопасности и конфиденциальности является программа обучения, которая помогает сформировать понимание рисков и объяснить роль каждого в выявлении, реагировании и управлении этими рисками. Несмотря на то, что программы обучения различаются в каждой федеральной организации, существуют фундаментальные общие элементы, которые могут быть использованы для создания стратегии Программы обучения кибербезопасности и конфиденциальности (CPLP) и обеспечения поддержки для внедрения, оценки и отчетности деятельности. Усилия CPLP вписываются в более крупную федеральную организационную программу по устранению рисков, включая усилия по снижению рисков, связанных с физической конфиденциальностью и безопасностью, инсайдерскими угрозами и другими связанными с этим проблемами управления рисками для человека. Такие усилия выходят за рамки настоящего документа.

Для удобства использования в оставшейся части настоящего документа термин «CPLP» будет использоваться для обозначения всех элементов осведомленности, обучения и образовательных мероприятий в области кибербезопасности и конфиденциальности, включая другие программы с такими названиями, как ознакомительные тренинги, практические упражнения (например, настольные учения, ролевые симуляции, киберполигоны или фишинговые кампании), тематическое обучение, ролевое обучение и образовательные программы. Организациям нет необходимости переименовывать свои программы в CPLP; Этот термин применяется в обобщенном смысле.

Предыдущая версия SP 800-50 определяла осведомленность, обучение и образование как отдельные элементы в непрерывном обучении. Исследования [[6]](#_bookmark107)[[7],](#_bookmark108) проведенные совместно с менеджерами по обучению федерального правительства, показали, что эти термины имеют разные значения и могут привести к путанице при описании более широкой цели создания CPLP. В то время как некоторые менеджеры могут называть программы «осведомленностью и обучением» или «обучением осведомленности», эти термины применяются непоследовательно в разных организациях. Независимо от того, как организация называет свою программу, всеобъемлющая цель CPLP заключается в предоставлении возможностей для обучения на всех уровнях или этапах карьеры. Речь идет о создании программ, где может происходить обучение.

В данной специальной публикации также используется термин «учащийся» для описания отдельных лиц в любом из сегментов аудитории учебной программы. Термин «учащийся» можно найти в SP 800-181r1 [[5]](#_bookmark106), где он относится к лицу, которое приобретает специализированные знания или развивает навык. Это определение полезно в данном случае, поскольку оно описывает всех участников «программы обучения». В этом документе программа будет называться CPLP или CPLP, поскольку в некоторых организациях может потребоваться несколько программ для удовлетворения требований к обучению всего персонала.

# Цель

Этот документ содержит рекомендации по созданию и поддержанию комплексных CPLP для федеральных организаций и включает в себя мероприятия и кампании по повышению осведомленности, тренинги по повышению осведомленности, практические упражнения, тематические тренинги, ролевые тренинги и образовательные программы. Документ включает в себя руководство о том, как организация может создать стратегический план программы и обеспечить наличие соответствующих ресурсов для достижения целей обучения организации.

Данное издание предназначено для обслуживания разнообразной аудитории, в том числе:

# Специалисты по кадрам и обучению

* + Лица, связанные с проектированием, разработкой, внедрением, оценкой, эксплуатацией, управлением и улучшением CPLP для федеральных агентств и организаций
  + Лица, ответственные за надзор за федеральными человеческими ресурсами, управлением талантами, подрядчиками и программами обучения
  + Лица, ответственные за федеральные CPLP, специалисты по обучению и менеджеры, такие как директора по обучению (CLO) и разработчики учебных программ

# Лидерство и управление

* + Лица, отвечающие за удовлетворение потребностей персонала в обучении, определение приоритетов использования учебных ресурсов, выявление пробелов в обучении и оценку эффективности обучения в рабочем пространстве
  + Лица, отвечающие за надзор за информационными системами или управление ими, такие как старшие руководители, менеджеры по рискам, уполномоченные должностные лица, директора по информационным технологиям (CIO), директора по информационной безопасности (CISO), сотрудники по управлению данными (DMO) и директора по конфиденциальности (CPO)
  + Лица, выполняющие обязанности по управлению кибербезопасностью и конфиденциальностью (например, управление программами и проектами и обеспечение того, чтобы сотрудники обладали соответствующими знаниями и навыками для выполнения своих рабочих ролей), включая руководителей программ и проектов, менеджеров по кибербезопасности и менеджеров по операциям по обеспечению безопасности

# Специалисты по кибербезопасности и конфиденциальности

* + Сотрудники, которые отвечают за оказание помощи в определении деятельности CPLP в качестве эксперта в предметной области (SME), выполнение требований ролей или должностных функций, выявление пробелов в обучении и/или компетенциях и потребностей в рамках программы кибербезопасности и конфиденциальности организации, определение необходимых настроек и разработку базового уровня соответствия для организации

**Ключевые соображения для руководителей федеральных программ обучения кибербезопасности и конфиденциальности**[4](#_bookmark6)

* Разработка, поддержка и внедрение обязательных CPLP в масштабах всей организации для всех сотрудников, которые поддерживают цели и задачи предприятия в области кибербезопасности и конфиденциальности.

4 Этот текст адаптирован из Циркуляра АБУ A-130, Приложение I, раздел 4.h, и предназначен для удовлетворения потребностей любой организации, а не только федеральных агентств и организаций.

* Убедитесь, что CPLP соответствуют установленным правилам поведения и соответствуют применимым политикам, стандартам и руководящим принципам.
* Информируйте сотрудников о доступных ресурсах кибербезопасности и конфиденциальности (внутренних и внешних), таких как политики, продукты, методы, передовые практики или экспертные знания.
* Обеспечить как базовый, так и более продвинутый уровни обучения сотрудников кибербезопасности и конфиденциальности, а также обеспечить принятие мер по оценке знаний и навыков участников.
* В консультации с высшим руководством определите модели поведения в области кибербезопасности и конфиденциальности, которые влияют на риски на основе данных.
* Определите тех, кто нуждается в специализированном обучении кибербезопасности и конфиденциальности на основе назначенных ролей и обязанностей в области кибербезопасности и конфиденциальности.
* Измеряйте отношение, поведение и настроения сотрудников в рамках отслеживания развития культуры кибербезопасности и конфиденциальности.

# Размах

В этом руководстве описывается, как федеральная организация может проектировать, разрабатывать, внедрять и поддерживать CPLP в рамках корпоративной программы кибербезопасности и конфиденциальности. Это включает в себя определение потребностей в обучении персонала организации, включая федеральных сотрудников, работающих полный или неполный рабочий день, стажеров, пенсионеров, подрядчиков, внешних партнеров, консультантов, исследователей и любых пользователей, которые получают доступ к корпоративной системе или данным в поддержку миссии организации.

CPLP включает в себя различные другие программы, такие как программы повышения осведомленности, кампании по социальной инженерии, обучение новых сотрудников, регулярное обучение, техническое обучение, обучение на основе ролей и другие соответствующие учебные мероприятия, проводимые внутри организации или через внешние ресурсы (например, курсы, сертификаты и продвинутые программы). Кроме того, CPLP являются частью более крупных федеральных организационных усилий по устранению и снижению рисков, связанных с угрозами физической конфиденциальности и безопасности, инсайдерскими угрозами и другими связанными с этим проблемами управления рисками, связанными с человеческим фактором. Эти усилия выходят за рамки данного документа.

# Жизненный цикл CPLP

CPLP должны иметь активно управляемые планы на протяжении всего их жизненного цикла, что требует внимания и корректировки с течением времени. Менеджеры CPLP должны тщательно и вдумчиво излагать, обсуждать, анализировать и документировать цели CPLP и имеющиеся варианты. Когда владельцы CPLP организации принимают эффективную стратегию и разрабатывают надлежащий подход к планированию с измерениями и обратной связью в течение года, вся организация остается на связи с

цели СПГС. [На рисунке 1](#_bookmark9) показаны ключевые этапы создания и управления программой обучения: Планирование и стратегия, Анализ и проектирование, Разработка и реализация, а также Оценка и улучшение.



**Рис 1. Жизненный цикл программы обучения по кибербезопасности и конфиденциальности**

Эти фазы могут протекать последовательно или одновременно. В любой момент жизненного цикла менеджеры CPLP и их команды могут разработать учебную программу, оценить отзывы инструкторов, разослать по электронной почте практические упражнения, разработать плакаты для повышения осведомленности или разработать презентацию для высшего руководства. Считайте эту схему напоминанием о широте работы.

В широком смысле CPLP являются ценными элементами культуры обучения организации. Чтобы быть эффективными, CPLP должны быть связаны с целями организации и рассматриваться как адаптивные, непрерывные и развивающиеся. В обучающейся организации персонал может расширить и улучшить свои текущие возможности для понимания и удовлетворения новых требований миссии. Персонал пользуется уважением за свою способность творить и вдохновлять других, а также активно участвует в достижении результатов обучения на протяжении всей жизни. Если организация предлагает другие программы обучения (например, развитие карьеры, лидерство и развитие руководителей), CPLP должны быть аналогичным образом интегрированы в структуру обучения в масштабах всего предприятия.

# Развитие культуры кибербезопасности и конфиденциальности

Развитие культуры кибербезопасности и конфиденциальности является важным компонентом создания успешной CPLP. Культура организации должна подчеркивать, подкреплять и направлять желаемое поведение в сторону кибербезопасности и конфиденциальности. Риски возрастают, когда доминирующая культура не признает ценность вовлечения людей в усилия по поддержке передовых практик кибербезопасности и конфиденциальности. Существует два сектора риска, которые CPLP может учитывать:

1. Технические риски — системы плохо спроектированы, не исправлены или аналогичным образом скомпрометированы по сравнению с идеальным состоянием. Эту проблему можно решить с помощью тематического и ролевого обучения, разработанного для практикующих специалистов с серьезными обязанностями в области кибербезопасности и/или конфиденциальности.
2. Риски, связанные с человеческим фактором — Люди не соблюдают свои стандарты кибербезопасности и конфиденциальности, или системы были плохо настроены и позволяют людям подвергать организацию неоправданным угрозам из-за различных человеческих ошибок.

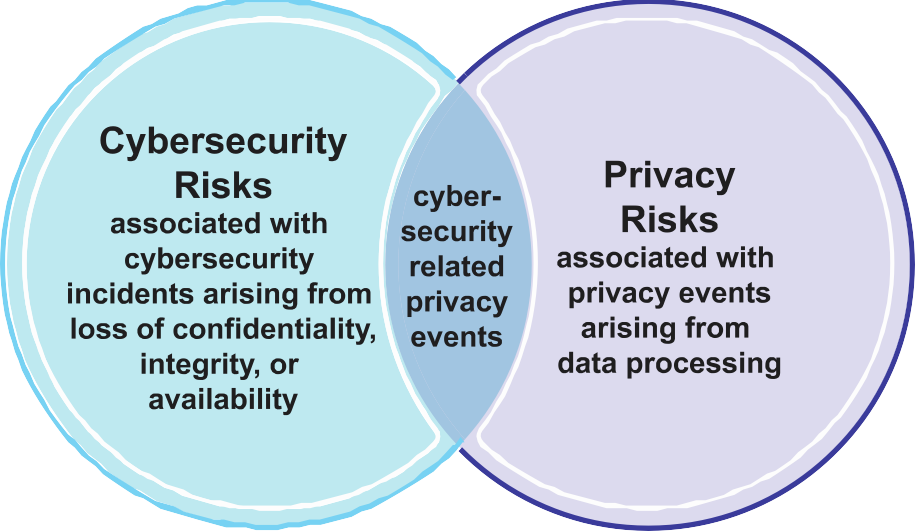
Когда CPLP ценится в культуре организации, способность учитывать оба типа рисков возрастает. Руководители организации устанавливают CPLP в качестве важного компонента управления рисками путем поддержки, продвижения и участия в учебных мероприятиях, от кампаний по повышению осведомленности до обучения на основе ролей. Менеджеры по обучению CPLP создают строгие системы измерения для оценки отношения сотрудников, вовлеченности и поддержки программы. Деятельность CPLP способствует и помогает измерить культуру кибербезопасности и конфиденциальности организации. Руководители отдела кадров укрепляют эти культурные нормы, гарантируя, что сообщения CPLP являются частью адаптации и других материалов на рабочем месте. В совокупности эти усилия задают тон всей организации.

Люди — это самый большой актив организации. Культура кибербезопасности и конфиденциальности поддерживает среду, в которой весь персонал хорошо разбирается в потребностях, ожиданиях и ценностях управления рисками кибербезопасности и конфиденциальности. Организация, в свою очередь, поддерживает эффективную культуру кибербезопасности и конфиденциальности, когда она понимает потребности сотрудников и проводит обучение и обучение, чтобы помочь сотрудникам и подрядчикам освоить ожидаемое поведение в области кибербезопасности и конфиденциальности. Любая эффективная учебная деятельность может быть включена в CPLP, если она уважительна, инклюзивна и помогает учащимся понять свою роль в организации. Содержание должно указывать учащемуся на то, что он является ценным участником, помогающим организации управлять рисками. Сотрудники ценят то, что они внесут свой вклад в позитивную культуру кибербезопасности и конфиденциальности организации с помощью знаний и навыков, которые они приобретут, участвуя в CPLP.

Организации и владельцы систем должны разработать подход CPLP, который отстаивает ответственность каждого пользователя за защиту информации и активов. Новые технологии и риски по-прежнему будут требовать общеорганизационного подхода к управлению рисками кибербезопасности и конфиденциальности. В NIST Cybersecurity Framework (CSF) [[8]](#_bookmark109), Privacy Framework [[9]](#_bookmark110) и Risk Management Management Framework (RMF) [[10]](#_bookmark111) подчеркивается важность осведомленности и обучения персонала, а также мониторинга и совершенствования методов управления рисками.

# Взаимосвязь между кибербезопасностью и неприкосновенностью частной жизни

Несмотря на то, что кибербезопасность и неприкосновенность частной жизни являются независимыми и отдельными дисциплинами, некоторые из их целей пересекаются. Программы кибербезопасности отвечают за защиту информации, информационных систем и операционных технологий от несанкционированного доступа, использования, раскрытия, сбоя, изменения или уничтожения (т. е. несанкционированной активности или поведения системы) с целью обеспечения конфиденциальности, целостности, доступности и безопасности. Программы обеспечения конфиденциальности отвечают за управление рисками для физических лиц, связанными с обработкой данных на протяжении всего жизненного цикла информации5[,](#_bookmark13)  с целью обеспечения предсказуемости, управляемости и разобщенности, а также соблюдения применимых требований к конфиденциальности. Управление рисками кибербезопасности способствует управлению рисками конфиденциальности. Тем не менее, одного управления рисками кибербезопасности недостаточно, поскольку риски конфиденциальности также могут возникать способами, не связанными с инцидентами кибербезопасности, как показано на [рисунке 2](#_bookmark12) [[9]](#_bookmark110).



**Рис 2. Взаимосвязь между рисками кибербезопасности и конфиденциальности**

Например, организация может объединить обезличенные данные с новым набором данных во время обработки данных, что приведет к повторной идентификации. Аналогичным образом, обезличенный набор данных может быть обнародован, но в сочетании с другой общедоступной информацией может привести к повторной идентификации. Действия по обработке данных не включают в себя инциденты или нарушения кибербезопасности, но все же представляют угрозу конфиденциальности.

Обучение сотрудников различным рискам кибербезопасности и конфиденциальности позволяет им эффективно бороться с рисками, с которыми они сталкиваются в своей повседневной деятельности. Например, всем сотрудникам потребуется обучение, которое поможет им понять, что такое событие конфиденциальности и как оно может произойти в их организации. Они должны иметь возможность идентифицировать событие конфиденциальности и сообщать о нем. Специалистам по реагированию на инциденты потребуется обучение, которое поможет им определить, когда инцидент кибербезопасности также может быть событием, связанным с конфиденциальностью, что часто требует дополнительных процедур при реагировании (например, определение того, привел ли незащищенный сайт к фактическому нарушению конфиденциальности).

5 Жизненный цикл информации описывает стадии, через которые проходит информация, такие как ее создание или сбор, обработка, распространение, использование, хранение и утилизация, включая уничтожение и удаление [[3].](#_bookmark104)

Организации могут извлечь выгоду из скоординированного и гибкого подхода к разработке CPLP, которые эффективно отвечают потребностям организации.[6](#_bookmark15)

Как только организация поймет взаимосвязь между кибербезопасностью и конфиденциальностью, она сможет определить свой подход к разработке как интегрированных, так и ориентированных на кибербезопасность или конфиденциальность учебных мероприятий на основе соответствующих тем и ролей сотрудников в своей среде. Например, организация может определить, как эффективно:

* Связывайте учебные курсы с рабочими ролями (особенно с обработкой данных) и производительностью труда
* Описать свой подход к управлению рисками кибербезопасности и конфиденциальности таким образом, чтобы он соответствовал возможностям управления рисками предприятия
* Учет уроков, извлеченных из рисков кибербезопасности и конфиденциальности, результатов аудита, инцидентов, событий или изменений в документах управления (например, законах, нормативных актах, политиках и стандартах) в общее и ролевое обучение
* Организуйте учебные мероприятия, подходящие как для внутренних, так и для внешних членов рабочей силы, включая подрядчиков и третьи стороны
* Определение обязательств по обучению в контрактах и соглашениях
* Определение и отслеживание метрик для оценки эффективности усилий по обучению (например, определение того, уменьшается ли количество инцидентов или событий определенного типа после целевой информационной кампании)

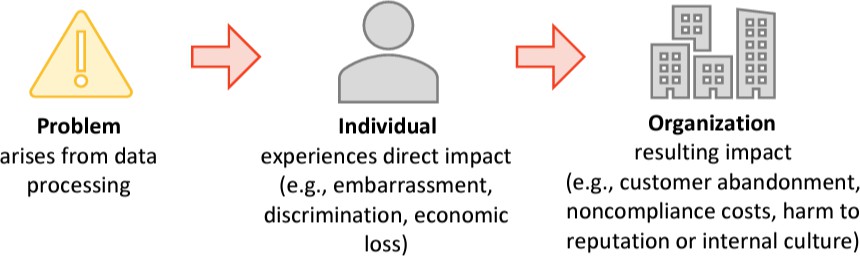
# Основные понятия управления рисками конфиденциальности

Сотрудники, чьи роли могут влиять на неприкосновенность частной жизни, также должны иметь четкое представление о том, как выявлять и устранять риски, которые могут возникнуть. NIST Privacy Framework [[9]](#_bookmark110) предоставляет общий язык для понимания, управления и информирования о рисках конфиденциальности. Так же, как сотрудники учитывают риски, связанные с событиями безопасности, они также должны учитывать *события конфиденциальности* — потенциальные проблемы, которые могут возникнуть в результате операций с системами, продуктами или услугами с цифровыми или нецифровыми данными на протяжении всего жизненного цикла, от сбора данных до утилизации. Проблемы с конфиденциальностью могут возникнуть в результате непосредственного использования продукта человеком. Некоторые проблемы также могут возникать просто из-за взаимодействия людей с системами, продуктами и услугами, даже если обрабатываемые данные напрямую не связаны с идентифицируемыми лицами. Проблемы, с которыми могут столкнуться люди в результате обработки данных, могут быть выражены по-разному. Концепция конфиденциальности NIST описывает их как варьирующиеся от достоинства

6 Обучение конфиденциальности на основе ролей должно охватывать весь спектр рисков, связанных с конфиденциальностью, как показано на рисунке 2. Для федеральных агентств обучение по вопросам конфиденциальности на основе ролей рассматривает типы информации, которые могут представлять собой информацию, позволяющую установить личность (PII), а также риски, соображения и обязательства, связанные с ее обработкой. В рамках такого обучения также учитываются полномочия на обработку данных, задокументированные в политиках и уведомлениях о конфиденциальности, уведомлениях о системе записей, соглашениях и уведомлениях о компьютерном сопоставлении, оценках воздействия на конфиденциальность, заявлениях Закона о неприкосновенности частной жизни, контрактах, соглашениях об обмене информацией, меморандумах о взаимопонимании или другой документации.

от последствий типа (например, смущение или стигматизация) до более ощутимого вреда (например, дискриминация, экономические потери или физический вред) [[9]](#_bookmark110).[7](#_bookmark19)

Физические лица могут столкнуться с проблемами конфиденциальности, возникающими в результате обработки данных, а организация, в свою очередь, может столкнуться с такими последствиями, как расходы на несоблюдение требований, потеря дохода из-за отказа клиентов от продуктов и услуг или ущерб репутации внешнего бренда или внутренней культуре. Организации обычно управляют этими типами воздействий на уровне управления рисками предприятия. Связывая проблемные действия с данными (т. е. действия по обработке данных, которые могут вызвать проблемы), с которыми сталкиваются отдельные лица, с этими хорошо понятными организационными последствиями, организации могут привести риски конфиденциальности в соответствие с другими рисками, которыми они управляют в своем более широком портфеле, и стимулировать принятие более обоснованных решений о распределении ресурсов для укрепления программ конфиденциальности. [На рисунке 3](#_bookmark16) показана взаимосвязь между рисками неприкосновенности частной жизни и организационными рисками [[9]](#_bookmark110).



**Рис 3. Взаимосвязь между рисками неприкосновенности частной жизни и организационными рисками**

CPLP наиболее эффективны, когда они помогают сотрудникам понять как прямое влияние событий конфиденциальности на отдельных людей, так и результирующее влияние, которое риски конфиденциальности могут оказать на организацию. Например, CPLP может охватывать типы последствий, которые физическое лицо может испытывать от вторичного использования данных (например, в маркетинговых целях) и вытекающие из этого последствия для организации (например, расходы, связанные с несоблюдением требований, потерей доверия к организации или изменением приоритетов миссии при устранении последствий).

# Координация усилий по обучению кибербезопасности и конфиденциальности

CPLP организации должна согласовываться с существующими программами кибербезопасности и конфиденциальности. В условиях ограниченных ресурсов дублирование усилий негативно скажется на одной или обеих программах. В тех случаях, когда существует интегрированная программа кибербезопасности и конфиденциальности, это вряд ли будет проблемой.

# Роли и обязанности

Хотя важно понимать политику, которая требует от агентств разработки и внедрения CPLP, организациям также важно понимать, кто несет ответственность за

7 Каталог NIST по проблемным действиям и проблемам, связанным с данными, содержит примеры проблем с конфиденциальностью, с которыми могут столкнуться физические лица, и доступен по адресу [https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM](https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md) [/catalog-PDAP.md.](https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md)

Обучение кибербезопасности и конфиденциальности. В этом разделе определены и описаны те сотрудники организации, которые отвечают за обеспечение доступа сотрудников к обучению кибербезопасности и конфиденциальности и его прохождению.

В SP 800-37r2 (редакция 2) *«Структура управления рисками для информационных систем и организаций: подход к жизненному циклу системы для безопасности и конфиденциальности*[» [10]](#_bookmark111) определены типичные роли, связанные с этими программами. Поскольку терминология может различаться в зависимости от организации, может быть полезно обратиться к Концепции NICE в качестве дополнительного инструмента для определения лиц, несущих ответственность за управление CPLP, и тех, кто нуждается в дополнительной подготовке. Публичная рабочая группа NIST Privacy Workforce (PWWG)[8](#_bookmark21) также располагает информацией о задачах, знаниях и навыках, необходимых для специалистов по конфиденциальности в организации.

Размер, зрелость и ресурсы CPLP могут сильно различаться, даже в пределах одной организации. Роли и обязанности на ключевых должностях в CPLP должны быть задокументированы, чтобы помочь обеспечить наиболее эффективное использование ресурсов и позволить программам дорасти до желаемого состояния. Таким образом, каждой организации необходимо подумать о том, как распределить эти роли. Независимо от того, выполняет ли один человек несколько функций или несколько человек сотрудничают в организации, помните о возможности дублирования обязанностей.

# Руководитель организационного отдела

Руководитель организации несет ответственность за защиту информационной безопасности и должен уделять приоритетное внимание разработке эффективных CPLP. Это включает в себя внедрение жизнеспособной программы кибербезопасности и конфиденциальности с сильным компонентом обучения. Как отмечается в СП 800-37r2, руководитель организации гарантирует, что «организация располагает надлежащим образом подготовленным персоналом для оказания помощи в соблюдении требований безопасности и неприкосновенности частной жизни, содержащихся в законодательстве, исполнительных указах, политиках, директивах, инструкциях, стандартах и руководящих принципах» [[10]](#_bookmark111). Руководитель организации должен:

* Назначение руководящих ролей для управления CPLP организации, разработка стратегического направления для программ обучения, формулирование целей и задач эффективности, а также анализ и управление показателями производительности. Менеджеры CPLP отвечают за анализ, разработку, разработку и реализацию CPLP и должны быть обеспечены достаточными ресурсами для достижения целей и задач в области деятельности.
* Обеспечить реализацию программы кибербезопасности и конфиденциальности в масштабах всего учреждения или организации; хорошо обеспечена ресурсами, включая персонал и финансирование; и эффективен в снижении рисков и управлении ими.
* Убедитесь, что агентство или организация располагает достаточным знанием и квалифицированным персоналом для поддержки своих программ и ресурсов и защиты частной жизни.
* Убедитесь, что поведение в области конфиденциальности и кибербезопасности, связанное с организационными рисками, выявляется и измеряется на основе данных.

8 Посетите веб-сайт Публичной рабочей группы NIST Privacy Workforce по адресу (PWWG) [https://www.nist.gov/privacy-framework/workforce-advancement](https://www.nist.gov/privacy-framework/workforce-advancement/privacy-workforce-public-working-group) [/privacy-workforce-public-working-group.](https://www.nist.gov/privacy-framework/workforce-advancement/privacy-workforce-public-working-group)

* Поддержка постоянного измерения культуры кибербезопасности и конфиденциальности.

# Высшее руководство

FISMA [[2]](#_bookmark103), Циркуляр OMB A-130 [[3]](#_bookmark104) и различные другие нормативные акты определяют ответственность за обеспечение CPLP для определенных старших должностных должностей. Названия этих должностей включают в себя исполнительного директора, заместителя директора, помощника директора, начальника отдела, директора по информационным технологиям, директора по конфиденциальности, директора по информационной безопасности, директора по данным, директора по искусственному интеллекту, владельца информации, владельца системы, владельца миссии или бизнеса, старшего ответственного должностного лица по управлению рисками и специалиста по безопасности системы или конфиденциальности. Эти роли отвечают за определение стратегического направления, выявление рисков и управление ими, обеспечение доступности ресурсов и надзор за персоналом, несущим значительную ответственность за кибербезопасность и конфиденциальность, включая роли, связанные с соответствующим финансированием и управлением программами.

Кроме того, высшее руководство должно отстаивать потребности в рабочей силе путем:

* Подавать пример и участвовать в собственном обучении CPLP, по мере необходимости
* Определение лиц, несущих ответственность за кибербезопасность и неприкосновенность частной жизни, и их документирование в должностных инструкциях или других соответствующих заявлениях о требованиях к работе и производительности.
* Определение актуальных требований к обучению и их документирование в индивидуальных планах развития или другой документации по карьерному росту
* Установление политик и процедур для программ обучения и их документирование в документах организации
* Если вы выполняете роль владельца системы или владельца данных, назначаете сотрудников, которые несут значительные обязанности по кибербезопасности и/или конфиденциальности в своей системе (например, в системах общей поддержки и основных приложениях), и гарантируете, что пользователи и вспомогательный персонал прошли соответствующее обучение тому, как выполнять свои обязанности, прежде чем им будет предоставлен доступ к системным ресурсам

Агентства и организации должны сформировать Комитет высшего руководства, который регулярно встречается с руководителями CPLP для обсуждения стратегии и предоставления ресурсной поддержки. Руководители СПЯС будут представлять Комитету высшего руководства регулярные отчеты о деятельности СПЯС в течение года. Если возникает риск или новая угроза, которую необходимо устранить в рамках CPLP, Комитет высшего руководства может связать учебную группу с оперативными группами и малыми и средними предприятиями, которые могут предоставить учебные материалы и ресурсы. Организации также могут включать представителей сотрудников в качестве заинтересованных сторон в Комитет высшего руководства, чтобы обеспечить им право голоса при принятии решений.

# Менеджеры CPLP

Менеджеры CPLP несут ответственность за CPLP на тактическом уровне. В этой роли менеджер CPLP должен работать со специалистами по разработке учебных программ и командой инструкторов, безопасностью

операционная группа, офицеры и менеджеры по безопасности информационных систем, директора по информационной безопасности, отделы кадров (HR), отделы закупок и управления рисками:

* Сотрудничество с малыми и средними предприятиями по вопросам политики в области толкования и применения соответствующего законодательства и организационной политики для руководства программой CPLP
* Содействие разработке учебных материалов, которые являются подходящими и своевременными для целевой аудитории
* Разработка эффективных подходов к распространению учебных материалов среди целевой аудитории для максимального вовлечения и воздействия
* Предложите учащимся и их руководителям эффективный способ предоставления обратной связи по учебному материалу и его подаче
* Контролируйте периодические обзоры и обновляйте учебные материалы по мере необходимости
* Обеспечение эффективного использования всех имеющихся внутренних и внешних ресурсов для эффективного управления СПЯС
* Помощь в разработке стратегии отслеживания и отчетности
* Помощь в выявлении лиц, несущих значительные обязанности в области кибербезопасности и конфиденциальности
* Предоставление высшему руководству регулярных отчетов о состоянии целей, задач и показателей эффективности CPLP

# Менеджеры

Термин «менеджеры» включает в себя руководителей и тех, кто несет организационные обязанности по обеспечению того, чтобы подчиненный им персонал соответствовал требованиям обучения кибербезопасности и конфиденциальности. Менеджеры должны:

* Работа с высшим руководством и менеджерами CPLP для выполнения общих обязанностей
* Создание индивидуальных планов развития (IDP) для оценки пробелов в знаниях персонала со значительными ролями и обязанностями в области кибербезопасности и конфиденциальности
* Содействие профессиональному развитию сотрудников, отвечающих за кибербезопасность и неприкосновенность частной жизни, и поощрение их к получению признанных в отрасли сертификатов
* Убедитесь, что персонал понимает конкретные правила каждой системы и приложения, которые они используют.
* Обеспечить, чтобы весь персонал (включая общий персонал) сохранял компетентность в области кибербезопасности и неприкосновенности частной жизни, участвуя в CPLP
* Работа над уменьшением ошибок и упущений со стороны персонала, которые могут быть вызваны недостаточной осведомленностью или обучением

# Пользователь системы

Пользователь системы – физическое лицо, уполномоченное на доступ к информации и информационным системам для выполнения возложенных на него обязанностей. Как отмечается в СП 800-37r2,

Обязанности пользователей системы включают, помимо прочего, соблюдение политик организации, которые регулируют приемлемое использование систем организации, использование предоставленных организацией ресурсов информационных технологий только для определенных целей, а также сообщение об аномальном или подозрительном поведении системы. [[10]](#_bookmark111)

# План и стратегия CPLP

Стратегический план CPLP дает представление о текущем состоянии обучения кибербезопасности и конфиденциальности в масштабах всей организации, о том, где организация хочет или должна быть, а также о том, как устранить разрыв между этими двумя состояниями (например, ресурсы, персонал). Стратегический план CPLP помогает менеджерам CPLP гарантировать, что персонал организации готов к решению проблем, связанных с рисками кибербезопасности и конфиденциальности, связанными с их работой.

Циркуляр АБУ A-130 [[3]](#_bookmark104) устанавливает общую политику планирования, бюджетирования, управления, приобретения и управления федеральной информацией, персоналом, оборудованием, фондами, ИТ-ресурсами, а также вспомогательной инфраструктурой и услугами. Каждое федеральное агентство обязано разработать, поддерживать и внедрять всеобъемлющую CPLP для удовлетворения потребностей своей миссии. Чтобы разработать надежную программу с разнообразными материалами, в том числе предлагающую учащимся увлекательные возможности быть в курсе актуальных рисков кибербезопасности и конфиденциальности для своей организации, CPLP должна иметь эффективную стратегию разработки, реализации и постоянного совершенствования.

В этом разделе обсуждаются шаги, связанные с созданием стратегического плана CPLP, который учитывает цели организации, уникальные требования, типы аудитории и объем программы. Этапы планирования также помогут организации оценить свои приоритеты, бюджет, ресурсы и коммуникационные планы.

# Построение стратегического плана

Стратегический план CPLP должен пересекаться со стратегическим планом организации по постоянному развитию рабочей силы. Владелец CPLP должен понимать структуру и миссию организации, чтобы определить, откуда берет начало стратегия организации. Некоторые агентства организованы по принципу «сверху вниз», когда штаб-квартира несет ответственность за миссию и дает рекомендации по стратегии CPLP. Другие организации разрабатывают CPLP в различных бизнес-функциях или комбинируют оба подхода. Документирование стратегии CPLP и того, как она способствует достижению целей стратегии управления рисками организации, показывает исполнительному руководству, почему CPLP необходима.

Хорошо разработанный стратегический план CPLP описывает, как управление рисками и культура кибербезопасности и конфиденциальности организации позволяют всем сотрудникам оценивать риски при каждом своем действии и решении. С агентствами разного размера программа, которая работает для одного, не обязательно будет работать для другого. Каждое агентство должно разработать программу, которая будет работать для него наилучшим образом. Стратегия СПЯС всегда должна быть четко сформулирована и, скорее всего, будет рассмотрена Комитетом высшего руководства и согласована до утверждения любого финансирования.

Стратегический план СПЯС должен охватывать ключевые вопросы, в том числе:

* Видение и миссия
* Стратегические цели и задачи
* Подходы к обучению и планы действий
* Тактики, которые помогают достичь поставленных целей
* Метрики и отчетность

Стратегический план СПЯС также должен:

* Опишите, как она поддерживает культуру принятия решений на основе оценки рисков, и подчеркните важность трансформационного обучения персонала, включая развитие знаний, навыков и способностей, чтобы помочь работникам добиться успеха сейчас и в будущем.
* Объясните, как программа будет восполнять пробелы в знаниях и навыках, расширять общие возможности и поддерживать культуру вовлечения персонала в их роли в области кибербезопасности и конфиденциальности.
* Пересекаются с общей миссией организации (например, формулировкой миссии и видения, толерантностью к риску, целями обучения, задачами, результатами, методами и организационной структурой)
* Включите информацию о политиках организации и владельцах политик, например о том, как существующие правила поведения, политики, процедуры и указания будут доведены до сведения персонала
* Включите метрики и измерения, которые помогают определить, достигают ли текущие программы целей и сохраняют ли учащиеся знания и навыки, меняют свое поведение и развивают позитивное отношение в поддержку культуры кибербезопасности и конфиденциальности.
* Включите операционную тактику, такую как инструменты, механизмы или методы, которые владельцы программы будут использовать для достижения целей программы
* Определите ключевых заинтересованных лиц, руководителей и роли, многие из которых будут работать в офисах ИТ-директора, директора по информационной безопасности, старшего сотрудника по информационной безопасности агентства (SAISO), старшего должностного лица агентства по вопросам конфиденциальности (SAOP), директора по маркетингу и отдела кадров
* Используйте результаты оценки рисков и существующие стратегии для обеспечения согласованности между разработкой программ, учебными материалами и управлением рисками
  + Существующие CPLP также могут извлечь выгоду из анализа пробелов или оценки текущей программы, чтобы четко провести различие между текущим и целевым состояниями и позволить руководству программы соответствующим образом сформировать свой подход.
* Определите, как программа будет соответствовать нормативным требованиям и нормативным требованиям для минимизации рисков, обучая персонал их роли в культуре кибербезопасности и конфиденциальности организации
* Планируйте и поддерживайте потребности разнообразной рабочей силы, в том числе с особыми потребностями, а также тех, кто работает удаленно или часто путешествует
* Включите методы обучения, которые являются эмпирическими и атомизируют контент (т.е. посмотрите, как существующий контент может быть разделен на более мелкие элементы или перепрофилирован)

# Разработка политики и процедур CPLP

Политика и процедуры CPLP работают вместе, чтобы выразить то, что организация хочет сделать и как это сделать. Политики — это ясные и простые утверждения, правила или утверждения, которые определяют правильное или ожидаемое поведение объекта. Они обеспечивают руководящие принципы для выполнения миссии и проведения операций, а также могут обеспечить последовательные и эффективные методы обучения и осведомления. Процедуры описывают, как будут реализовываться или вводиться в действие политики. Они составляются с учетом того, кто и что будет делать, шаги или фазы действия, определенные критерии или уровни реализации, а также сопутствующая документация.

Для бизнес-операций в области кибербезопасности и конфиденциальности политики и процедуры определяют приемлемые практики и ожидания, а также рекомендации по обучению персонала этим требованиям и ожиданиям. Политика и процедуры CPLP должны соответствовать более широкой политике организации и четко описывать ожидания от программ обучения.

Преимущества создания политик и процедур включают в себя:

* Четкие ожидания в отношении персонала во всей организации
* Документально оформленная поддержка программы со стороны руководства
* Возможности управления и надзора с возможностью проведения аудита
* Определение стратегических целей и задач в области кибербезопасности и обеспечения конфиденциальности
* Четко определенная информация и ресурсы CPLP
* Структурированный подход к обучению персонала их обязанностям в области кибербезопасности и неприкосновенности частной жизни
* Документирование эволюции культуры кибербезопасности и конфиденциальности

# Примеры заявлений о политике программы обучения

В следующих примерах заявлений о политике представлен контекст того, что важно при установлении, пересмотре или обновлении политик CPLP.

* ИТ-директор и директор по информационной безопасности должны разработать программу обучения кибербезопасности для пользователей информационных систем [организации].
* CPO должен разработать программу обучения по вопросам конфиденциальности для пользователей данных [организации].[9](#_bookmark30)
* Все сотрудники, подрядчики или другие лица, работающие от имени [организации], имеющие доступ к системам [организации], должны пройти первоначальное обучение и регулярное повышение квалификации по вопросам кибербезопасности и конфиденциальности, а также принятых методов кибербезопасности и конфиденциальности

9 Циркуляр OMB A-130 [[3]](#_bookmark104) включает в себя обязанности по защите федеральных информационных ресурсов и управлению PII. Тем не менее, каждая федеральная организация может выбрать другой язык для обозначения того же понятия. Этот документ соответствует Концепции конфиденциальности NIST и использует термин «данные» для обозначения информации, связанной с обработкой данных о физических лицах. Организациям следует проконсультироваться со своими юридическими консультантами, чтобы определить предпочтительный язык.

* Персонал должен пройти обучение по кибербезопасности и конфиденциальности в течение 24 часов с момента получения учетной записи пользователя. Если пользователь не выполнит это требование к обучению, доступ к нему не будет предоставлен или будет приостановлен.
* Все сотрудники, подрядчики или другие лица, работающие от имени [организации] и выполняющие значительные обязанности по обеспечению безопасности, должны пройти обучение на основе ролей до получения доступа к системам, обрабатывающим конфиденциальную информацию, и должны будут проходить повторное обучение каждый финансовый год.
* Учетные записи пользователей и права доступа, включая доступ к электронной почте, должны быть отключены для сотрудников, которые не прошли необходимое переобучение, если только CISO, представители CISO или менеджер по безопасности информационных систем (ISSM) не предоставили разрешение на это.
* Менеджеры по конфиденциальности, директора по информационной безопасности и ISSM должны подготовить и представить необходимые планы обучения на основе осведомленности и ролей.
* Менеджеры по конфиденциальности, директора по информационной безопасности и ISSM должны готовить и представлять отчеты об изменениях в поведении сотрудников, мерах отношения и других показателях, связанных с развитием культурных норм кибербезопасности и конфиденциальности, с содержанием, частотой, форматом и распространением по запросу CPO и CIO.
* Директор по информационной безопасности или его представители должны регулярно пересматривать программы обучения на основе осведомленности об информационной безопасности и ролевые тренинги.

SP 800-53r5 [[11]](#_bookmark112) control AT-1 описывает политики и процедуры для программ повышения осведомленности и обучения (обучения) в области кибербезопасности и конфиденциальности.

# Согласование стратегий, целей, задач и тактик

Организации могут использовать различные методы для определения и описания шагов, необходимых для реализации программы. Один из методов заключается в том, чтобы начать с определения целей организации, задач для достижения этих целей и оперативной тактики для достижения этих целей. Каждая цель должна иметь задачи, которые часто включают в себя измеримые задачи, такие как определение тех, кто нуждается в обучении на основе ролей, или обучение определенного процента организации к определенной дате. Рекомендуется выбирать «УМНЫЕ» цели: конкретные, измеримые, достижимые, актуальные и ограниченные по времени. Каждая цель программы будет иметь тактику, связанную с ней. Тактика – это инструменты, методы или механизмы, которые позволяют программе преследовать цель, определенную в стратегии плана. В конечном счете, каждый отдельный пункт плана — вплоть до самого детального тактического уровня — может быть прослежен до того места, откуда он берет начало в общей стратегии. Каждое мероприятие должно поддерживать общую стратегию CPLP. Управление этапами внедрения CPLP и обеспечение того, чтобы программа соответствовала потребностям организации в обучении, требует дисциплины со стороны команды.

[В таблице 1](#_bookmark32) представлена модель стратегии, включая цели, задачи и тактику.

**Таблица 1. Элементы стратегии CPLP**

|  |  |
| --- | --- |
| **Элемент** | **Описание** |
| **Стратегический план** | Менеджеры CPLP встречаются для установления или пересмотра приоритетов и разработки стратегического плана CPLP. |
| **Стратегические цели** | Определите отдельные элементы стратегического плана, вокруг которых будет организована программа, такие как снижение восприимчивости к атакам с использованием социальной инженерии, определение сроков применения мер по управлению рисками конфиденциальности, более широкое внедрение многофакторной аутентификации или  Учебные мероприятия на основе сценариев. |
| **Цели** | Исходя из стратегических целей, разработайте цели, которые включают в себя отчетливые измеримые результаты и типы показателей, связанных с программным элементом. |
| **Тактика** | Исходя из поставленных целей, разработайте тактику для частичного или полного достижения целей программы, например, упражнение по фишингу для повышения осведомленности об атаках социальной инженерии, общекорпоративные информационные бюллетени или другие средства объявления, вебинары по многофакторной аутентификации.  основы и процедуры, или мозговой штурм с малыми и средними предприятиями по разработке сценариев. |

Следующие два сценария демонстрируют каждый из этапов реализации.

# Сценарий 1: Защита конфиденциальных печатных данных

Анализ физической безопасности той части организации, где многие сотрудники регулярно обрабатывают конфиденциальные данные, показывает, что основные шаги для поддержания «чистого рабочего места» не предпринимаются. Политика конфиденциальности требует, чтобы файлы, содержащие конфиденциальные данные, хранились в папках в запираемых шкафах. Во время проверки распечатанные файлы, содержащие конфиденциальные данные, были расположены в стопках бумаг и папках, которые были небрежно размещены на столах.

Менеджер CPLP стремится улучшить работу с распечатанными конфиденциальными данными и обеспечить соблюдение персоналом требований защиты. Они определяют, что свежая, привлекающая внимание информационная листовка или плакат могут способствовать лучшему соблюдению сотрудниками политики и снизить этот риск.

Руководитель предлагает доступное финансирование, предназначенное для производства печатной продукции. Менеджер CPLP может использовать эти средства для печати наклеек «Keep It Clean», которые прикрепляются к рабочим папкам и предоставляют кейс таких папок каждому сотруднику в области, которая обрабатывает конфиденциальные данные.

В этом примере менеджер CPLP постоянно контролировал рабочее место и риски, координировал бюджет, планировал печать наклеек и работал с руководством для доставки материалов. Поскольку это разовая проблема, этапы планирования были оптимизированы в рамках существующей программы.

* ***Стратегический план —*** соблюдение требований к конфиденциальности.
* ***Стратегическая цель —*** Поддержка программы конфиденциальности организации.
* ***Цель —*** Обеспечить, чтобы все сотрудники, работающие с конфиденциальными данными, прошли обучение и знали о своих обязанностях по обеспечению конфиденциальности.
* ***Тактика —*** Предоставьте наклейки «Keep It Clean» для папок в тех частях организации, где обрабатываются конфиденциальные данные.

# Сценарий 2: Разработка новой программы обучения, соответствующей нормативным требованиям

Новый регламент требует, чтобы все специалисты по кибербезопасности внедрили определенную процедуру в свою повседневную жизнь.

Менеджер CPLP работает с владельцами политик кибербезопасности, чтобы понять и интерпретировать регламент. Вместе они определяют стратегию с целями, задачами и набором тактик программы, чтобы обеспечить новое обучение для всех членов рабочей силы и удовлетворить новые требования с помощью конкретных новых процедур. Менеджер CPLP решает работать с организационным персоналом, обучающим его, чтобы создать онлайн-опыт, который также позволит удаленным работникам в полной мере участвовать в этом.

По мере завершения курса менеджер CPLP работает с руководителями организации и руководством, чтобы определить ожидаемые показатели завершения и успеха, а также обеспечить выявление и обучение всех необходимых членов рабочей силы. В качестве элемента непрерывного мониторинга менеджер CPLP работает с учебным офисом и руководством для проверки завершения и успешности обучения.

* ***Стратегический план —*** дать возможность всем специалистам по кибербезопасности осознать свою ответственность и развить необходимые навыки для соответствия новым нормативным требованиям.
* ***Стратегическая цель —*** обновление обучения для всех специалистов по кибербезопасности в соответствии с новыми нормативными требованиями.
* ***Цель —*** Запустить (или обновить) программу онлайн-обучения, которая позволит всем специалистам по кибербезопасности достичь целей обучения по конкретной процедуре в новых правилах, даже находясь на удаленной работе.
* ***Тактика —*** Работа с руководством над планированием обучения и обеспечением 100% соответствия, а также разработка программы непрерывного мониторинга для проверки показателей выполнения и предоставления ежедневных данных отслеживания менеджерам.

# Определение измерений и метрик CPLP

Программные измерения и метрики являются ключевыми факторами на этапе оценки и совершенствования жизненного цикла CPLP (см. разд. [пункт 1.3](#_bookmark8)). Измерения CPLP позволяют организации описать и количественно оценить программу обучения, показать эффективность и влияние программы, понять, где для успеха требуются изменения, удовлетворить потребности в бюджете и ресурсах, а также принять решения на основе данных. Благодаря разработке и мониторингу измерений CPLP организация может лучше решать свои цели обучения и использовать ресурсы.

Для целей CPLP необходимо различать количественные и качественные измерения. Количественное измерение оценивается путем присвоения объекту номера или категории для описания атрибута этого объекта, например, с использованием шкалы от 1 до 5 для оценки эффективности учебного контента. Например, инструкция по оценке программы после обучения может гласить: «Оцените свой уровень знаний о подвигах социальной инженерии по шкале от 1 до 5, где 1 — низкий уровень знаний, а 5 — высокий уровень знаний». Такое измерение позволяет оценить содержание обучения по среднему или среднему баллу.

Качественное измерение основано на описательных данных, например, данных, собранных в ходе наблюдений, интервью, фокус-групп или открытых текстовых полей в опросах.

# Измерения

Разработка и внедрение измерений CPLP требует тщательного рассмотрения и должно определяться целями и задачами программы, а также любыми нормативными требованиями. Менеджеры CPLP должны быть готовы ответить на некоторые распространенные вопросы, такие как:

* Какие законы, политики и нормативные акты применяются к нашей организации?
* Как часто требуется отчетность?
* Какие данные должны быть включены в отчет?
* Какие данные для потенциальных аудитов мы должны хранить и в течение какого времени?

Менеджер CPLP должен определить, как будут собираться измерения, как часто, кто должен иметь доступ к измерениям, а также как отчеты будут документироваться и распространяться. В то время как законы, нормативные акты и политики часто устанавливают конкретные измеримые требования, измерения CPLP должны выходить за рамки простого обеспечения соответствия. Влияние CPLP на возможности рабочей силы, отношение и изменения в поведении также должно быть измерено.

Измерения и метрики должны быть непосредственно связаны с целями, *задачами* и *результатами* обучения по программе и организации CPLP. Хотя эти термины часто используются как взаимозаменяемые, каждый из них имеет определенное значение в отношении обозначения и сбора измерений и метрик. Будь то на организационном уровне, на уровне курса, модуля или урока, эти термины сохраняют свои различные значения. Для пояснения в этом документе приводятся следующие высокоуровневые определения этих терминов и описывается, как они используются в учебном сообществе:

* **Цель: Цель** – это общее заявление, написанное с точки зрения организационной или учебной команды, которое описывает предполагаемую компетенцию и желаемые задачи, знания и/или навыки, которые участник получит в ходе мероприятия.
* **Цель: Цели** представляют собой конкретные утверждения, написанные с точки зрения организации или учебной группы, которые описывают, что разработчик хочет, чтобы участник делал после завершения учебной деятельности. Цели обычно относятся к конкретному предмету или содержанию, которое будет охватываться учебным материалом.
* **Результат:** Результаты обучения ориентированы на учащегося и описывают, как будет оцениваться учащийся. Письменные результаты обучения должны быть измеримыми, достижимыми и основанными на результатах. Общая формула для записи результатов обучения выглядит следующим образом:
  + После участия в учебном упражнении учащиеся смогут (*вставить измеримый глагол*) и (*вставить учебное утверждение*).

[В таблице 2](#_bookmark37) приведены примеры целей, задач и результатов обучения, а также то, как их различия влияют на создание измерений для программы.

**Таблица 2. Примеры целей, задач и результатов обучения**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Учебный семестр** | **Перспектива** | **Метод оценки** | **Измерение** | **Метод измерения (количественный и количественный)**  **качественный)** |
| **Цель:** Помочь учащимся понять преимущества использования утвержденных инструментов генеративного искусственного интеллекта (ИИ), которые имеют отношение к их работе  роль | Организация, команда по разработке инструкций или инструктор | Оценивается организацией или учебной командой путем изучения учебного содержимого | Дало ли содержание курса учащимся понимание преимуществ использования ИИ? | Обратная связь от докладчиков и программ, открытые опросы, отчеты от участников |
| **Цель:** Научить учащихся (1) определять утвержденные инструменты генеративного ИИ, (2) выбирать подходящий инструмент генеративного ИИ, который имеет отношение к их рабочей роли, и (3) использовать утвержденный инструмент генеративного ИИ для повышения эффективности своей работы  Обязанности | Организация, команда по разработке инструкций или инструктор | Оценивается организацией или учебной командой путем изучения учебного содержимого | Рассматривались ли в учебных материалах инструменты генеративного ИИ? Были ли критерии принятия решений представлены рабочими ролями? Были ли представлены преимущества для каждого инструмента ИИ? | Обратная связь с докладчиками и программой, открытые опросы, отчеты участников, наблюдения за участниками программы обучения |
| **Результат:** Обучение учащихся доступу к утвержденным инструментам генеративного ИИ и создание деятельности с использованием генеративного ИИ, соответствующей их рабочей роли | Ученик | Оценивается организацией или учебной группой для определения способности учащегося продемонстрировать свои новые знания или навыки | Смог ли учащийся получить доступ к инструментам ИИ и использовать их для создания задания с использованием ИИ? | Интерактивные оценки, викторины, лабораторные демонстрации, устные оценки и наблюдения за учебной программой  Участников |

Менеджеры CPLP должны создавать программы с эффективными методами сбора данных для предоставления эффективной отчетной информации. Это, вероятно, будет включать в себя сбор данных о сотрудниках, которые могут иметь повышенную конфиденциальность из-за контекста (например, записи об обучении часто являются частью записей о занятости или контракте и могут быть связаны с оценкой производительности или приводить к последствиям в случае непрохождения необходимого обучения). Менеджеры CPLP должны выявлять и управлять рисками кибербезопасности и конфиденциальности, связанными с обработкой данных обучения, включая риски, связанные с системами управления обучением (LMS) и практикой отчетности.

# Количественные измерения

Количественные измерения выражаются в числовой форме и обычно называются объективными данными. Сочетание количественных и качественных измерений обеспечивает целостное понимание CPLP.

Некоторые распространенные примеры данных программ количественного обучения включают:

* Посещаемость тренингов, оценка производительности и процент завершенных курсов
* Обратная связь по закрытому опросу сотрудников
* Стоимость разработки и доставки в расчете на одного участника
* Использование онлайн-программ или других цифровых программ обучения, таких как количество входов в систему, время, проведенное в Интернете для доступа к контенту, и частота доступа к сайту или контенту.
* Отслеживание количества участников, которые пытались получить коммерческую сертификацию и получили ее
* Данные об инцидентах кибербезопасности ограничены инцидентами, созданными сотрудниками, или темами, которые могут быть смягчены или рассмотрены в учебных программах
* Метрики отчетности об инцидентах, демонстрирующие способность сотрудников распознавать потенциальные события кибербезопасности и сообщать о них
* Отслеживание реакции на фишинг или другую имитацию атаки
* Продольные данные, отражающие влияние программы, включая изменение поведения сотрудников, с течением времени (например, своевременное внедрение сотрудниками обновлений операционной системы, более широкое внедрение многофакторной аутентификации, соблюдение правил управления паролями)
* Тестирование данных сотрудниками до программы обучения, сразу после программы обучения и через три месяца после посещения курса для оценки усвоения знаний
* Данные о производительности по отделам, включая технические измерения производительности
* Периодичность обновления обучающего материала для оценки актуальности
* Масштабы событий кибербезопасности или конфиденциальности, такие как сокращение времени простоя или простои из-за событий (это могут быть индикаторы для обучения на основе ролей)
* Способность распознавать и сообщать о раскрытии или неправомерном использовании информации о конфиденциальности, о чем свидетельствует принятие сотрудниками инструментов отчетности
* Изменения, внесенные после технического обучения, также могут обеспечить такие измерения, как сокращение числа счетов с привилегированным доступом, выявление ценных активов, новая сегментация сети или дополнительные меры контроля, описанные в документации по закупкам и бюджету

# Качественные измерения

Качественные измерения основаны на описательных данных, например, данных, собранных в ходе наблюдений, интервью, фокус-групп или открытых текстовых полей в опросах, и могут дать представление об учебном процессе*.*

Некоторые распространенные примеры данных о качественных программах обучения включают:

* Наблюдения и отзывы преподавателей/докладчиков
* Опросы об отношении персонала к культуре кибербезопасности и конфиденциальности
* Открытые поля обратной связи или опроса
* Подробные отчеты от участников, такие как письменные отзывы, отправленные в программу
* Обсуждения в фокус-группах с участниками, преподавателями или другими заинтересованными сторонами
* Наблюдения за обучением, обучением и взаимодействием
* Наблюдения и анализ учебных кейсов
* Интервью с участниками, инструкторами или другими заинтересованными сторонами
* Отправка ящиков для предложений

# От измерений к метрикам

Разработка показателей может быть одной из самых важных, но сложных частей работы CPLP. То, как организация определяет и собирает измерения, приведет к определению и анализу показателей. Эффективный набор показателей может помочь улучшить качество контента и вовлеченность учащихся, получить поддержку от организации, увеличить финансирование, выявить влияние на программу управления рисками кибербезопасности и конфиденциальности, а также продемонстрировать отдачу от инвестиций. В недавнем исследовании программ обучения, проведенном NIST, участники сообщили [[6],](#_bookmark107) что, несмотря на лучшие намерения, их организации часто использовали ограниченное количество показателей, которые не давали полного представления об эффективности программы.

В следующих примерах показано, как измерения предоставляют данные для метрик: Посещаемость курса

* Метрика: процент учащихся, которые зарегистрировались и посетили учебный курс
* Измерения: Регистрация и учет посещаемости (количественные)
* Анализ: Выявление различий или тенденций в том, сколько зарегистрированных учащихся и сколько присутствовавших

Завершение курса

* Метрика: процент и характеристики учащихся, завершивших учебный курс
* Измерение: количество учащихся, их рабочие роли и организация, которые посетили и завершили курс (количественно)
* Анализ: Выявление различий или тенденций в том, сколько учащихся приняли участие и сколько из них завершили курс

Вовлеченность во время курсов

* Метрика: уровень взаимодействия с участниками, например, сколько из них участвовали в обсуждениях или завершили интерактивные элементы
* Измерение: количество учащихся, принявших участие в групповых или лабораторных занятиях (количественные данные), комментарии и отзывы, полученные от учащихся (качественные), а также количество участников, задавших вопросы или участвовавших в функциях чата (количественные)
* Анализ: Определите тенденции на основе того, сколько учащихся приняли участие в мероприятиях по вовлечению и были ли положительные или отрицательные отзывы участников о мероприятии

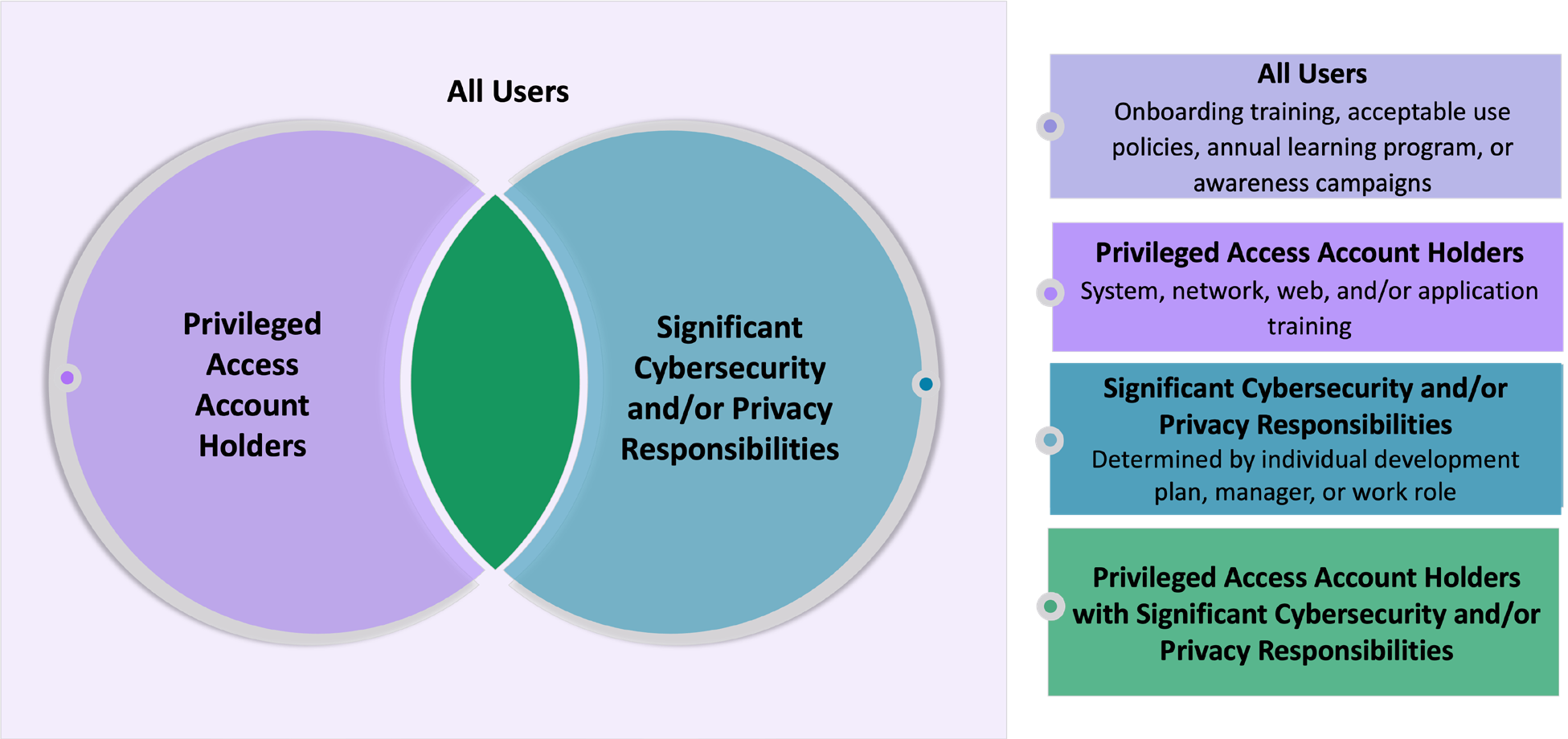
Стоимость курса на одного участника

* Метрика: стоимость программы по сравнению с количеством участников, посетивших курс
* Измерение: стоимость курса (количественная) и количество посетивших курс (количественная)
* Анализ: Определение экономической эффективности путем сравнения посещаемости и затрат Изменение поведения в расчете на одного участника
* Метрика: процент участников, которые изменили поведение на рабочем месте (например, сообщили о подозрительном фишинговом электронном письме)
* Измерение: количество участников, которые получили электронное письмо от теста на фишинг и сообщили о нем надлежащим образом (количественно)
* Анализ: Определите влияние обучения на распознавание фишинговых писем и то, как о них сообщается

Менеджеры CPLP полагаются на измерения и метрики CPLP для оценки эффективности своих программ обучения и обеспечения достижения результатов обучения. SP 800-55v1 [[12]](#_bookmark113) содержит рекомендации по выбору и агрегированию измерений информационной безопасности, а также по разработке программы измерений информационной безопасности.

# Сегменты аудитории программы обучения

При рассмотрении персонала организации, чьи цели обучения будут решаться с помощью CPLP, рекомендуется рассматривать каждого человека как принадлежащего к одному или нескольким сегментам аудитории программы обучения. Каждый человек, участвующий в CPLP, учитывается в группе «все пользователи». Ко второй группе относятся владельцы учетных записей с привилегированным доступом, которые имеют одобренный организацией доступ к системам с ограниченным доступом или данным, требующим особой осторожности. Эти лица пройдут дополнительное обучение по кибербезопасности и конфиденциальности, чтобы свести к минимуму риски для систем и данных. В третью группу входят сотрудники и подрядчики со значительными обязанностями в области кибербезопасности и/или неприкосновенности частной жизни, которым требуется индивидуальная программа ролевого обучения, чтобы гарантировать, что их знаний и навыков достаточно для выполнения задач, необходимых для их работы. Вероятно, будет некоторое совпадение между владельцами учетных записей с привилегированным доступом и теми, кто несет значительные обязанности в области кибербезопасности и/или конфиденциальности. [На рисунке](#_bookmark40) [4](#_bookmark40) показаны группы и то, как они перекрываются.



**Рис 4. Сегменты аудитории обучающей программы CPLP**

# Все пользователи

В типичном сценарии все сотрудники организации будут участвовать в CPLP, соглашаться соблюдать политику допустимого использования или стандарты поведения, проходить обучение по повторяющейся программе обучения, а также посещать, завершать, просматривать и получать другие различные элементы текущей программы.

SP 800-53r5 [[11]](#_bookmark112) Управление AT-2, Awareness and Training, относится к обучению «всех пользователей» как обучению «грамотности» в области кибербезопасности и конфиденциальности. В рамках или после завершения повторяющегося обучения пользователи подписывают политику правил поведения, определяющую поведение, необходимое для получения и сохранения доступа к системе. SP 800-53r5 также указывает, что обучение необходимо будет обновлять в связи с любыми изменениями в системе или после любых событий, определенных организацией:

Последующее обучение грамотности может быть удовлетворено одним или несколькими короткими специальными занятиями и включать в себя тематическую информацию о последних схемах атак, изменениях в политике безопасности и конфиденциальности организации, пересмотренных ожиданиях в отношении безопасности и конфиденциальности или подмножестве тем из первоначального обучения. Регулярное обновление материалов по обучению грамоте и повышению осведомленности помогает гарантировать, что контент остается актуальным. События, которые могут ускорить обновление материалов по обучению грамотности и повышению осведомленности, включают, помимо прочего, результаты оценки или аудита, инциденты или нарушения безопасности, а также изменения в применимых законах, исполнительных указах, директивах, правилах, политиках, стандартах и руководствах.

Все пользователи (обычно называемые «системными пользователями» и «обычными пользователями») имеют решающее значение для уменьшения количества непреднамеренных ошибок и уязвимостей. Сотрудники организации могут

10 Федеральные агентства и организации должны обращаться к текущим требованиям FISMA для определения частоты программ «Все пользователи».

К ним относятся сотрудники, занятые полный и неполный рабочий день, подрядчики, консультанты, иностранные или отечественные приглашенные исследователи, посетители, гости, другой персонал агентства и другие сотрудники или партнеры, которым требуется доступ. Все пользователи должны:

* Понимать и соблюдать политики и процедуры организации в области кибербезопасности, физической безопасности и конфиденциальности
* Понимать и принимать правила поведения для систем и приложений, к которым у них есть доступ
* Работа с руководством для удовлетворения потребностей в обучении
* Быть в курсе действий, которые они могут предпринять для лучшей защиты информации и окружающей среды своей организации

Примеры тем, которые могут рассматриваться в CPLP, включают:

* Понимание того, как деятельность в области кибербезопасности и конфиденциальности поддерживает миссию и бизнес-цели организации
* Использование правильных паролей или многофакторной аутентификации
* Обработка данных
* Использование искусственного интеллекта или других корпоративных инструментов
* Изучение процедур удаленного доступа
* Сбор и защита персональных данных
* Сообщение о любых предполагаемых инцидентах или нарушениях политик кибербезопасности и конфиденциальности
* Следование правилам, установленным для предотвращения атак социальной инженерии (например, программ-вымогателей и фишинга) и предотвращения распространения спама и вредоносного ПО.
* Выявление и устранение рисков конфиденциальности при обработке информации
* Знание того, где найти ресурсы организации по кибербезопасности и конфиденциальности, а также точки контакта

Организация также может иметь возможность выявлять тех, кто подвержен или кто представляет больший риск для человека из-за своей роли, используемых приложений или просто потому, что они еще не взяли на себя обязательство внедрить передовые методы кибербезопасности и конфиденциальности. Менеджер CPLP — в консультации с индивидуальным руководителем и ИТ-отделом — должен разработать дополнительные механизмы для выявления рискованного поведения и метрики для оценки участия в программе обучения «всех пользователей», а также рассмотреть способы стимулирования изменения поведения позитивными, а не карательными способами.

# Владельцы учетных записей с привилегированным доступом

Лицам с учетными записями с привилегированным доступом доверяется дополнительный доступ или обязанности для выполнения функций, которые обычные пользователи не имеют полномочий, таких как настройка управления сетью и предоставление доступа к системе (например, привилегии системного администрирования). Должный

Чтобы иметь доступ к критически важным ресурсам, владельцам учетных записей с привилегированным доступом требуется дополнительное обучение, чтобы убедиться, что они понимают свои привилегии доступа к учетной записи и не могут случайно вызвать или использовать уязвимости или неправомерное использование данных. Для каждого типа учетной записи с привилегированным доступом менеджер CPLP должен координировать обучение с менеджером или руководителем владельца учетной записи, сотрудником по персоналу и менеджерами по обучению, чтобы обеспечить проведение и поддержание актуальности обучения.

# Сотрудники, выполняющие значительные обязанности в области кибербезопасности и/или неприкосновенности частной жизни

Сотрудники, выполняющие значительные обязанности в области кибербезопасности и/или конфиденциальности, в том числе некоторые владельцы учетных записей с привилегированным доступом (например, «суперпользователи»), имеют права или доступ к конфиденциальным или критически важным системам и нуждаются в дополнительном обучении. Например, менеджер HR-среды, который следит за правильной конфигурацией и доступностью системы, или директор по персоналу (CHCO), который участвует в разработке политик для системы, будет нести значительную ответственность за кибербезопасность и конфиденциальность. Сетевые и ИТ-администраторы, управляющие системой и доступом к сети, являются владельцами учетных записей с привилегированным доступом. Если их рабочие роли включают мониторинг потери данных или другие вопросы конфиденциальности и кибербезопасности, то они также несут значительные обязанности по кибербезопасности и/или конфиденциальности, которые требуют дополнительного обучения на основе ролей. Этот доступ может быть аннулирован при изменении рабочей роли владельца.

SP 800-53r5 [[11]](#_bookmark112) управление AT-3, Role-Based Training, дает определение требуемого обучения:

Комплексное обучение на основе ролей охватывает управленческие, операционные и технические роли и обязанности, охватывающие физический, кадровый и технический контроль. Обучение на основе ролей также включает в себя политики, процедуры, инструменты, методы и артефакты для определенных ролей безопасности и конфиденциальности. Организации проводят обучение, необходимое для выполнения ими своих обязанностей, связанных с операциями и управлением рисками в цепочке поставок в контексте программ безопасности и конфиденциальности организации. Обучение на основе ролей также распространяется на подрядчиков, которые предоставляют услуги федеральным агентствам.

Это обучение обычно связано с должностными обязанностями, определенными руководителями организации (например, ИТ-директором, CPO или CISO агентства) и менеджером или руководителем сотрудника, и документируется в плане выполнения работы сотрудника. Персоналу, занимающему эти должности, может потребоваться профессиональное развитие для поддержания своего статуса или членства, например, ежегодные сертификации или курсы. Примерами типичных получателей обучения на основе ролей являются директор по информационной безопасности, специалисты по конфиденциальности, менеджеры по кибербезопасности, аналитики кибербезопасности и конфиденциальности, а также специалисты по реагированию на инциденты.

Рабочие роли и компетенции в области кибербезопасности исследуются в SP 800-181r1 [[5]](#_bookmark106), в котором описываются знания, навыки и задачи, связанные с работой, связанной с кибербезопасностью.

# Определение того, кто несет значительную ответственность за кибербезопасность и/или неприкосновенность частной жизни

FISMA [[2]](#_bookmark103) требует, чтобы персонал, выполняющий значительные обязанности в области кибербезопасности и/или конфиденциальности, проходил обучение на основе ролей. Дополнительные указания можно найти в SP 800-37r2 [[10]](#_bookmark111), SP 800-53r5

[[11]](#_bookmark112), и SP 800-181r1 [[5]](#_bookmark106). В совокупности эти документы помогают определить роли и функции в рабочей силе кибербезопасности, требующие ролевого обучения.

Определение того, кто в организации будет участвовать в обучении на основе ролей, представляет собой многоступенчатый процесс, который начинается с определения важных рабочих ролей в области кибербезопасности и конфиденциальности в организации и выявления сотрудников, которые соответствуют назначенным рабочим ролям. Часто решение начинается с высшего руководства и указаний из офиса CIO, CISO или CPO в партнерстве с HR. Менеджеры CPLP должны активно участвовать в этой работе, чтобы выявить тех, кто несет значительную ответственность за кибербезопасность и конфиденциальность.

Эти рабочие роли также должны быть включены в описания должностей, иерархические диаграммы и обязанности, чтобы показать, как была определена работа, необходимая для достижения конкретной цели. Люди могут брать на себя дополнительные рабочие роли в зависимости от своих конкретных навыков, организационной политики в отношении перекрестного обучения и уровня укомплектованности персоналом организации. СП 800-181р1

[[5]](#_bookmark106) определяет рабочие роли в области кибербезопасности и представляет собой подробный лексикон для понимания соответствующих знаний и навыков, типичных для таких ролей.

# Определение объема и сложности

Конечной целью CPLP является снижение рисков кибербезопасности и конфиденциальности для организации за счет культурных и поведенческих изменений, а не просто достижение соответствия.

Сложность материала должна быть определена до начала освоения и быть соизмерима с ролью человека, который будет проходить обучение. Материал должен разрабатываться на основе двух важных критериев: 1) роль целевого участника и 2) обязанности в области кибербезопасности и конфиденциальности, необходимые для этой роли. Для этого потребуется координация с HR и CLO (или аналогичными). Лица, прошедшие обучение, по достоинству оценят усилия, приложенные для того, чтобы убедиться, что они понимают материал в соответствии с их потребностями в обучении и характером выполняемой ими работы.

# Элементы CPLP

Типичная CPLP включает в себя множество элементов учебной программы, которые предоставляются различным аудиториям с помощью различных платформ и методов. Менеджеры CPLP определят необходимые и наиболее эффективные типы элементов программы для каждого типа аудитории для каждой цели обучения и скорректируют их выбор в соответствии с имеющимся бюджетом и соображениями по графику.

Типичными элементами CPLP являются:

* Мероприятия по повышению осведомленности
* Экспериментальное обучение и практические занятия
* Тренировка

Первоначально сотрудники могут считать, что CPLP — это ежегодный или регулярно запланированный учебный курс или мероприятие, проводимое для всех пользователей, которое может включать в себя неформальные программы отдела, обязательную презентацию в аудитории или онлайн-курс. Прочее обучение

Элементы программы предназначены для тех, кто несет значительные обязанности в области кибербезопасности и/или конфиденциальности, а также для тех, кто является владельцем учетных записей с привилегированным доступом. Программа CPLP будет состоять из обязательных элементов (требуемых политикой и целями обучения для всех участников обучения CPLP) и многих других мероприятий, реализуемых на протяжении всего жизненного цикла CPLP для закрепления этих идей.

Независимо от учебной деятельности, учебная цель этих мероприятий заключается в том, чтобы убедиться, что персонал осознает свою роль и ответственность за защиту информации и активов и способен принимать соответствующие меры для реагирования на различные риски кибербезопасности и конфиденциальности.

# Упражнения по повышению осведомленности

Учебные мероприятия по кибербезопасности и конфиденциальности должны проводиться на постоянной основе в течение года, чтобы сотрудники знали о своей роли в организации и о соответствующих шагах, которые они должны предпринять для защиты информации, активов и частной жизни. Мероприятия могут быть ориентированы на кампанию или проводиться спонтанно в зависимости от темы, угроз или уязвимостей, а также проводиться во время сезонных событий.

Примеры мероприятий по повышению осведомленности, подходящих для всех пользователей, включают:

* Сообщения на экранах входа в систему, заставках организации и блоках подписи электронной почты
* Информационные бюллетени для сотрудников со статьями о кибербезопасности и конфиденциальности
* Плакаты (физические или цифровые) с советами по кибербезопасности и конфиденциальности
* Ярмарка мероприятий «Месяц осведомленности о кибербезопасности» (октябрь) или «Неделя осведомленности о конфиденциальности данных» (январь)
* Напоминания о кибербезопасности и конфиденциальности, а также советы по материалам для сотрудников (например, ручкам, блокнотам и т. д.)
* Периодические или по мере необходимости сообщения электронной почты со своевременными советами или в ответ на событие или проблему в области кибербезопасности или конфиденциальности

# Эмпирическое обучение

Экспериментальные учебные мероприятия или практические упражнения — это конкретные сценарии обучения, которые имитируют события и инциденты. Практические упражнения могут включать в себя усилия по социальной инженерии (например, фишинг, смишинг и вишинг) в форме симуляций, обучающих игр, викторин по идентификации и обработке данных, настольных упражнений, практических виртуальных лабораторных упражнений, планов действий в чрезвычайных ситуациях и сценариев аварийного восстановления, а также сценариев атаки или защиты, проводимых в кибердиапазонах.

Например, в рамках общеорганизационного учения по борьбе с фишингом всем пользователям пользователям отправляется «хитрое» электронное письмо, чтобы узнать, смогут ли они обнаружить попытку фишинга или их можно обмануть, заставив перейти по ссылке на вредоносный веб-сайт или открыть зараженное вложение. Упражнения по фишингу также могут быть нацелены на обучение тех, кто занимает определенные должности, например руководство или известные администраторы. Начните с определения текущего коэффициента кликов для определенной группы пользователей или по рабочим ролям, чтобы понять, есть ли необходимость в более целенаправленном обучении. Шкала NIST Phish Scale может быть полезна для идентификации

и измерение поведения на предмет фишинговых угроз.[11](#_bookmark51) Эти упражнения дают возможность собирать метрики и измерения, которые обычно называются «кликами» или отчетными измерениями. Эти типы измерений показывают, сообщил ли пользователь о письме как о попытке фишинга, перешел ли он по ссылке или открыл вложение. Некоторые организации включают в свою почтовую платформу функцию «Сообщить о фишинге» (например, кнопку в меню платформы), чтобы продвигать передовые методы.

Юридическая команда организации должна быть включена в разработку и анализ запланированных мероприятий по фишингу, чтобы избежать негативных последствий, таких как использование законных брендов или упоминание федеральных организаций в качестве фишинговой «приманки», что может привести к электронным письмам или звонкам в эти организации. Кроме того, поскольку сотрудникам может не нравиться, когда их обманывают, важно сообщить им, что организация проводит учения по фишингу на случайной основе и что результаты будут использованы для руководства будущими учебными мероприятиями. Эти действия не должны носить карательный характер, и ни один сотрудник не должен быть привлечен к ответственности. Если рассматривать упражнения по фишингу как возможность обучения, они могут предоставить важные данные об уязвимостях и о том, какие сотрудники могут нуждаться в дополнительной поддержке в обучении.

Другие упражнения на основе опыта могут лучше подходить для тех, кто несет значительные обязанности в области кибербезопасности или конфиденциальности (например, ролевое обучение), такие как командно-штабные учения и сценарии плана действий в чрезвычайных ситуациях. Дополнительные примеры можно найти в NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities [* [13]](#_bookmark114).

# Содержание тренинга

Обучение — это широкий термин, который включает в себя содержание программы обучения, предназначенную для увеличения или улучшения знаний и навыков, связанных с работой. Некоторые из методов, которые может использовать организация, включают:

* **Синхронное обучение:** Преподаватели и учащиеся участвуют вместе в виртуальной или физической учебной среде в классе.
* **Асинхронное обучение:** учащийся может получить доступ к материалам индивидуально и по запросу. Иногда это называется «самостоятельным темпом», потому что учащийся получает доступ к контенту в соответствии со своим расписанием.
* **Виртуальное руководство:** обучение происходит в виртуальной или смоделированной среде и представляется или проводится инструктором в режиме реального времени.
* **Киберполигон:** Обучение проходит в безопасной учебной среде на основе веб-технологий (т.е. в песочнице) и обеспечивает практическое реалистичное обучение, сценарии, задачи и упражнения.
* **Подкасты:** обучение происходит асинхронно, в индивидуальном темпе и основано на аудио.
* **Анимация:** Анимация может визуально представлять процесс, систему или сложную концепцию кибербезопасности или конфиденциальности.

11 Шкала фишинга NIST учитывает контекст сотрудника в своем методе определения сложности смоделированного фишингового электронного письма. Дополнительную информацию смотрите <https://doi.org/10.6028/NIST.TN.2276> .

* **Демонстрация:** Преподаватель предоставляет учащемуся пошаговые действия процесса или деятельности. Это может быть доставлено лично, в записи или с помощью других методов.
* **Упражнение на основе сценариев:** фасилитатор ведет обсуждение тематических, ситуационных сценариев, которые могут быть адаптированы к организации или конкретному отделу. Их также называют «настольными» упражнениями.
* **Самостоятельное онлайн-обучение:** Этот асинхронный метод в настоящее время популярен в распределенных средах. Участники веб-сеанса могут учиться самостоятельно и учиться в своем собственном темпе. Функции тестирования и подотчетности могут измерять производительность. Веб-обучение может включать в себя видео, аудио и интерактивные методы, такие как перетаскивание или заполнение пропусков на экзамене.
* **Обучение под руководством инструктора на месте:** Это один из старейших и наиболее популярных методов донесения учебных материалов до аудитории. Самым большим преимуществом этой методики является интерактивный характер обучения. Он также может включать в себя презентации коллег и наставничество.

Сочетание различных методов проведения тренингов может быть эффективным способом презентации материала и удержания внимания аудитории. Например, показ видео во время сеанса под руководством инструктора позволяет аудитории сосредоточиться на другом источнике информации. Видео также может закрепить то, что представлял инструктор.

# Установление приоритетов плана СПЯС

На этапе планирования жизненного цикла CPLP оцените критические факторы риска организации, чтобы определить приоритеты обучения. Если поэтапный подход необходим из-за бюджетных ограничений или нехватки ресурсов, следует учитывать следующие факторы:

* **Роль и организационное влияние —** очень распространено рассмотрение приоритетов с точки зрения организационных ролей и рисков. Инициативы по повышению осведомленности на широкой основе, направленные на выполнение задач в масштабах всего предприятия, могут получить высокий приоритет, поскольку правила надлежащей практики кибербезопасности и конфиденциальности могут быть быстро доведены до сведения сотрудников. Также принято рассматривать  *должности с высоким уровнем доверия/высоким влиянием* (см. разд. [1.6](#_bookmark18)) и обеспечить, чтобы они получили высокий приоритет в стратегии развертывания. Эти типы должностей обычно соизмеримы с типом доступа, которым обладают эти пользователи, или специализированными требованиями, назначенными для их ролей и должностных обязанностей. Кроме того, защита ценных или критически важных активов или развертывание продуктов или услуг, чувствительных к конфиденциальности, также могут определять приоритеты.
* **Состояние текущего соответствия —** Это включает в себя рассмотрение основных пробелов в CPLP (например, анализ пробелов) и выявление недостающих областей, требующих внимания.
* **Доступность материалов и ресурсов —** Определите, имеются ли подходящие учебные материалы и необходимые ресурсы для элемента программы. По возможности перепрофилируйте и используйте существующие материалы новыми способами.

# Разработка плана CPLP

План CPLP определяет достаточно подробные программные элементы, которые поддерживают стратегию для каждого вида деятельности или кампании. Многие организации используют стандартные шаблоны планов программ, которые обеспечивают исходные показатели ожиданий организации. Точный уровень детализации плана будет варьироваться в зависимости от организационных и программных требований, а также ресурсов. По мере развития программы руководитель CPLP должен проводить периодические (т.е. не реже одного раза в год) обзор плана вместе с заинтересованными сторонами и отдельными лицами, которые будут поддерживать и управлять программой.

# Ресурсы CPLP

Важным элементом разработки стратегии CPLP является определение того, что в настоящее время существует в организации и какие ресурсы выделяются на существующие программы. Если программа обучения еще не существует или требует существенной переработки или обновления, обратитесь к процессу разработки стратегии программы (описанному в. [2.1](#_bookmark27)) рассмотреть наиболее важные элементы программы для включения. Ресурсы обычно определяются как любые активы, необходимые для достижения целей и задач, такие как люди, материалы, оборудование и технологии. Важным фактором при получении ресурсов является составление бюджета СПЯС.

# Определение бюджета СПЯС

После того, как стратегия CPLP была одобрена высшим руководством (указано в разд. [1.6.2](#_bookmark22)) и установлены приоритеты, потребности в финансировании должны быть добавлены в план. Необходимо принять решение о том, какой объем финансовой поддержки будет выделен, исходя из стратегических целей. Высшее руководство должно помочь менеджеру CPLP понять или составить свой бюджет. Хотя у каждой программы будут разные потребности в финансировании, некоторые типичные расходы включают в себя:

* Обучающий персонал, такой как менеджеры программ, дизайнеры учебных курсов, инструкторы, художники-графики, веб-разработчики и программисты
* Пространство в классе и материалы, такие как доски, маркеры, ластики, флипчарты, блокноты, ручки, карандаши и карточки с именами.
* Печатные программные материалы, раздаточные материалы и сертификаты или электронное распространение, для которого могут потребоваться веб-платформы
* Онлайн-пространство (т. е. виртуальное) пространство для распространения материалов, включая синхронные мероприятия (например, вебинары) и асинхронные действия (например, вспомогательные материалы, записанные сеансы и веб-контент)
* LMS для доставки контента, регистрации участников и записей о прохождении курса
* Лицензии (за рабочее место) для учебных платформ или контента
* Информационные материалы, такие как плакаты, блокноты и тематические предметы для информационных мероприятий
* Профессиональные услуги по проектированию и разработке учебных программ и презентации контента
* Усилия по составлению карты культуры конфиденциальности и кибербезопасности

Организации с ограниченным (или даже отсутствующим) бюджетом на инициативы в области кибербезопасности и конфиденциальности все же могут установить эффективную CPLP, используя существующие ресурсы, внедряя экономичные решения для мониторинга и уделяя приоритетное внимание кибербезопасности и конфиденциальности в качестве общей ответственности в масштабах всей организации. Некоторые материалы могут быть доступны в других федеральных агентствах, партнерских организациях или на онлайн-ресурсах поставщиков. Некоторые материалы могут уже существовать внутри компании и должны быть инвентаризированы и оценены, чтобы определить, являются ли они актуальными и соответствуют ли существующим целям обучения. График реализации поможет определить, когда может потребоваться дополнительное финансирование для поддержки инструментов, основных учебных программ и материалов, новых требований к персоналу и других элементов и мероприятий программы обучения.

Ниже приведены примеры вопросов, которые могут помочь в разработке бюджетных требований:

* + Какая миссия и потребности бизнеса будут затронуты или затронуты?
  + Существуют ли нормативные акты, законодательные требования или другие внутренние или внешние требования, которые могли бы повлиять на решение?
  + Какие общие федеральные или иные внешние ресурсы могут быть привлечены?
  + Какие внутренние ресурсы можно использовать? Это может включать в себя существующий контент и средства доставки.
  + Является ли экономически более экономически выгодной разработка материала собственными силами или аутсорсинг?
  + Является ли требование к обучению специфичным для организации или системы? Это включает в себя политику, процедуры или правила поведения.
  + Когда учебный материал должен быть готов? Есть ли критически важные графики, которые необходимо выполнить? Позволит ли аутсорсинг соблюсти графики поставок?
  + Сколько человек необходимо обучить?
  + Как часто нужно будет обновлять материал?
  + Какие средства доставки потребуются и каковы связанные с этим расходы?
  + Есть ли внутренние ресурсы для выполнения этой работы?
  + Обладает ли организация знаниями в предметной области, чтобы предоставить контент для обучения?
  + Имеются ли ресурсы для эффективного управления и мониторинга деятельности подрядчиков во время закупок?
  + Исключает ли чувствительность курса использование подрядчика?
  + Какова стоимость рабочего времени персонала и как CPLP может достичь желаемых результатов, максимизируя при этом отдачу от инвестиций (ROI)?

Менеджеры CPLP должны работать с высшим руководством, чтобы отстаивать программу против конкурирующих приоритетов, бюджетных ограничений и затрат времени персонала, а также разрабатывать стратегию для устранения любого дефицита финансирования, который может повлиять на способность организации достичь своих целей в области обучения. Для этого может потребоваться корректировка стратегии обучения в соответствии с имеющимся бюджетом, пропаганда дополнительного финансирования или перераспределение текущих ресурсов. Это также может означать, что план программы должен быть поэтапно введен в действие в течение некоторого заранее определенного периода времени по мере поступления финансирования.

# Персонал и местонахождение CPLP

Те, кто руководил федеральными CPLP, сообщают, что обучение рабочей силы требует сочетания технических знаний и профессиональных качеств, таких как коммуникативность, креативность и навыки межличностного общения [[7](#_bookmark108)]. Если у организации нет бюджета на разработку курсов CPLP, изучите, что сделали другие агентства или организации аналогичного размера для удовлетворения своих собственных потребностей. В некоторых организациях могут быть штатные дизайнеры учебных программ, разработчики учебных программ, инструкторы, веб-разработчики, эксперты по коммуникациям и графические дизайнеры. Другим организациям может потребоваться включить эти профессиональные расходы в бюджет нового проекта и найти квалифицированных подрядчиков или внешние курсы.

Разная информация требует разных способов доставки. Некоторые элементы программы будут подходить для онлайн-обучения, в то время как другие потребуют как инструкторов, так и физического расположения аудиторий. Определение этих требований на этапе планирования позволит соответствующим образом распределить ресурсы (например, зарезервировать помещения, обеспечить безопасность компьютеров и проекторов и т. д.). Даже плакаты и флаеры требуют экономии места, так как они должны быть размещены на достаточно видном месте, чтобы оказать обучающее воздействие на персонал.

# Информирование о стратегическом плане и результативности программы

Одним из наиболее важных аспектов реализации стратегического плана CPLP является сотрудничество с учебной группой, ключевыми заинтересованными сторонами, высшим руководством и персоналом. Вовлечение заинтересованных сторон и сотрудников в процесс планирования может привести к большему успеху в начале программы и по мере реализации каждого ее элемента. При определении того, о чем следует сообщать, следует сосредоточить внимание на:

* Как CPLP помогает в достижении организационных целей и целей обучения
* Как элементы CPLP повлияют на персонал
* Взаимодействие с заинтересованными сторонами для заблаговременного выявления проблем или конфликтов
* Получение обратной связи для выявления пробелов или недостающих элементов в плане
* Поддержка текущих усилий по развитию культуры кибербезопасности и конфиденциальности Получение ранней и постоянной поддержки стратегического плана важно для сохранения

импульс для СПЯС сильный и вдохновляет на вовлечение и удовлетворенность планом. Надежная коммуникационная стратегия удовлетворит эти потребности. Подумайте, есть ли в организации централизованный отдел коммуникаций или решения по коммуникациям будут приниматься на уровне бизнес-подразделений. Затем разработайте план коммуникаций (или включите эти элементы

в существующий план коммуникаций) для обмена информацией о новом или обновленном CPLP. Сделайте его простым и адаптированным к внутренним заинтересованным сторонам. Менеджер CPLP может выбрать создание пользовательской версии стратегического плана, которая включает в себя различную информацию для разных аудиторий.

Некоторые важные элементы, которыми следует поделиться, включают информацию о том, что такое CPLP и кто им управляет. Также может потребоваться выявление и устранение проблем и пробелов в финансировании. Например, руководители и менеджеры агентств должны знать, будут ли затраты на реализацию мероприятий CPLP финансироваться из бюджета CCI, CISO, CLO или другого программного бюджета, или это повлияет на их бюджеты, чтобы покрыть часть расходов. Кроме того, должны быть сообщены графики и требования к завершению.

Коммуникационный план CPLP должен включать:

* Обзор стратегии и ответственности CPLP
* Цели, задачи и процессы оценки
* Список ключевых ролей и их соответствующих обязанностей, в том числе:
  + Высшее руководство и руководители
  + Менеджеры и супервайзеры
  + Отдел кадров, Офис CHCO и трудовые отношения
  + Офис финансового директора (CFO) или бюджетного аналитика
  + CLO (уровень агентства или организации)
  + Менеджеры и члены команды CPLP
  + Малые и средние предприятия
* Обзор бюджета
* Ключевые результаты и высокоуровневый график
* Измерения и метрики
* Методы и периодичность представления отчетности

Все, кто участвует в реализации программы, должны понимать свои роли и обязанности. Большинству организаций может быть полезно адаптировать свои сообщения в зависимости от аудитории. Вот несколько примеров аудитории и ее ролей:

* **Высшее руководство и руководители** (например, директор, директор по информационным технологиям, директор по информационной безопасности, saiso, saop, caio и CPO)

**—** Сообщения могут включать в себя краткое изложение стратегического плана CPLP, включая цели и этапы годовой программы. Высшее руководство должно понимать общую программу, чтобы оно могло поддерживать распределение бюджета и персонала. Убедитесь, что высшее руководство получает надлежащую информацию, чтобы они могли избегать вредоносных формулировок (например, «пользователи — самое слабое звено»).

* **Менеджеры и супервайзеры —** Коммуникации должны подчеркивать преимущества создания позитивной культуры кибербезопасности и конфиденциальности и помогать менеджерам и руководителям

признать их решающую роль в поддержке этой культуры. Поощряйте положительные ассоциации с выделением времени для обучения сотрудников.

* **Специалисты по персоналу, управлению человеческим капиталом и должностные лица по трудовым отношениям — Лица,** занимающиеся персоналом или человеческим капиталом, несут ответственность за любые необходимые коммуникации относительно внедрения требований CPLP при адаптации и обучении сотрудников и подрядчиков в течение года. В организациях, членами которых являются члены профсоюза, сотрудники по трудовым отношениям также будут ключевыми заинтересованными сторонами в оказании помощи в любых обновлениях плана и получении отчетов о результатах обучения и других показателях для персонала, представленного профсоюзом. Человеческий капитал также является важнейшей заинтересованной стороной для внесения вклада в дисциплинарные меры персонала и, при необходимости, для инициирования трудовых отношений и переговоров с профсоюзом в отношении обязательного обучения или обучающих мероприятий, предусмотренных в процессе агентства.
* **Финансовый директор (CFO) —** Офис финансового директора (или эквивалентный ему старший финансовый директор организации или агентства) отвечает за утверждение CPLP и распределение финансирования менеджеру CPLP и, следовательно, должен быть информирован о реализации программы и измерениях.
* **Chief Learning Officer (CLO) —** CLO отвечает за образование в организации и может предоставлять учебную инфраструктуру, такую как LMS или другие платформы распространения.
* **Персонал —** Создайте коммуникационную стратегию, которая позволяет отправлять прямые сообщения по электронной почте персоналу и распределенную систему их менеджерам и руководителям. При создании информационных материалов о CPLP для отдельных сотрудников (например, материалов в пакетах ориентации для новых сотрудников) сосредоточьте усилия на том, чтобы дать возможность отдельным сотрудникам увидеть свою роль в общей CPLP. Это должно включать в себя расписание, гарантирующее, что пользователи будут уведомлены заблаговременно до того, как они должны будут завершить учебную деятельность.

# Анализ и проектирование CPLP

Несмотря на то, что существует множество теорий и моделей для проектирования и разработки учебных программ, в этом документе основное внимание уделяется модели ADDIE[12](#_bookmark60) — традиционной модели проектирования учебных систем с пятью различными этапами:

1. Анализ
2. Проектировать
3. Развитие
4. Реализация
5. Оценка

На этапе анализа менеджер CPLP выявляет организационные потребности и потребности в обучении или пробелы, чтобы определить, какая аудитория будет нуждаться в обучении, а также их текущий уровень знаний и навыков. Может возникнуть необходимость в оценке различных рабочих ролей на предмет пробелов в компетенциях, чтобы можно было адаптировать и создать соответствующие программы обучения на основе конкретных потребностей в обучении и навыках для этой рабочей роли. На этапе проектирования эти пробелы преобразуются в цели обучения, которые находятся в центре внимания учебного материала. Привязка целей обучения к выявленным пробелам в знаниях и навыках гарантирует, что конечный результат будет актуальным и позволит успешно удовлетворить выявленные потребности в обучении.

# Фаза анализа

Фаза анализа — это процесс, в ходе которого менеджер CPLP определяет потребности организации в обучении и производительности. В этом контексте потребности (т.е. пробелы) – это разница между текущими целями обучения (или видами деятельности) и желаемым состоянием. Чтобы определить свои потребности в обучении, организации могут проводить формальную или неформальную оценку потребностей (также называемую анализом потребностей). Основное преимущество этапа анализа заключается в определении потребностей организации и обучающейся аудитории в обучении. К дополнительным преимуществам относятся наличие информации, которая четко определяет потребности в обучении, поддержка и приоритизация ресурсов, а также согласование целей обучения с целями миссии организации.

В начале этапа анализа может быть полезно определить основных членов аналитической группы, включая несколько дополнительных составляющих групп. Это может включать:

* **Исполнительное руководство —** Эти организационные лидеры должны понимать соответствующие правила, директивы, законы, оперативные изменения или другие требования, которые составляют основу CPLP. Важно, чтобы руководство вносило свой вклад в удовлетворение потребностей организации в обучении, поскольку оно определяет ожидания от программы и учащихся. Ключевая роль менеджеров CPLP заключается в том, чтобы постоянно отстаивать программу, объясняя, почему анализ важен и как эффективный CPLP является частью эффективного управления рисками. Кроме того, эффективная и хорошо продуманная CPLP поддерживает

12 Модификация этой модели добавляет «Планирование» в качестве первого шага, что делает ее моделью PADDIE. Может быть полезно использовать модели, которые помогают в управлении изменениями или используют подходы, ориентированные на человека или человека. Все они имеют ценность и должны использоваться, когда это уместно для конкретной среды, организации и желаемого результата обучения.

Развитие организационной культуры, ориентированной на кибербезопасность и защиту конфиденциальности.

* **Персонал по кибербезопасности и конфиденциальности —** эти лица выступают в качестве малых и средних предприятий и консультантов организации. Они выявляют и помогают документировать знания и навыки, необходимые для выполнения задач, связанных с рабочими ролями.
* **Владельцы систем и менеджеры программ —** эти лица будут обладать информацией и ответственностью за конкретную систему, используемую организацией. Например, владелец системы будет осознавать потенциальное влияние учебной деятельности на персонал, которому поручено работать с этой системой.
* **Участники или учащиеся программы обучения —** представители сотрудников и различных должностных ролей в области кибербезопасности и конфиденциальности могут внести свой вклад в процесс сбора и анализа требований.

# Важность этапа анализа

Существует множество причин, по которым фаза анализа выполняется в спешке или вообще пропускается. Например, организации могут думать, что это займет слишком много времени, персонал может отсутствовать или может отсутствовать необходимое финансирование. Чаще всего организации считают, что они уже знают, что им нужно. Однако при пропуске этапа анализа могут возникнуть критические проблемы, такие как:

* Напрасные траты средств при разработке учебных материалов, которые не соответствуют требуемым пробелам в знаниях или навыках.
* Непонимание пробелов в знаниях и навыках учащихся, для устранения которых может потребоваться персонал, технологии или другие ресурсы.
* Использование обучения для решения проблемы, которая не является пробелом в знаниях или навыках (например, сотрудник не может выполнять «дополнительные обязанности по назначению»). Проведение анализа поможет определить, является ли это систематическим или структурным разрывом, а не пробелом в знаниях или навыках.
* Предоставление нужному персоналу неверной информации, например, предоставление владельцам учетных записей с привилегированным доступом только базового обучения, а не информации, относящейся к их дополнительным правам.
* Предоставление нужной информации неправильному персоналу, например, обучение владельцев учетных записей с привилегированным доступом для обычных пользователей.
* Предоставление правильной информации с помощью неэффективного средства или предоставление неверной информации с помощью эффективного средства.
* Повторение одного и того же учебного материала, даже если предыдущие попытки не увенчались успехом.

Может возникнуть соблазн пропустить время, необходимое для надлежащего анализа потребностей организации. Даже если единственным вариантом является проведение неформального обсуждения и обзора с несколькими людьми, все равно важно провести разговор и задокументировать то, что необходимо. На этапе анализа формируется четкое видение следующих шагов развития CPLP.

# Этапы этапа анализа

Несмотря на то, что существует множество способов, с помощью которых менеджеры CPLP могут оценить потребности организации в обучении, процесс определения потребностей программы обучения со стратегической точки зрения, как правило, является повторяемым процессом, независимо от конкретной цели обучения или аудитории. Шаги следующие:

1. Определение потребностей в обучении на основе рабочих ролей, действий и задач
2. Определите аудиторию программы обучения
3. Сопоставляйте выявленные потребности в обучении с каждой аудиторией
4. Оцените текущие знания и уровень навыков аудитории
5. Определите пробелы в обучении

# Определите потребности в обучении

Наиболее важным шагом в начале нового этапа в CPLP является определение потребностей в обучении. Например, организация может быть готова к внедрению новых технологий, может быть принят закон, требующий от персонала приобретения новых знаний или навыков, или может возникнуть новый риск конфиденциальности или кибербезопасности, который потребует от организации внедрения нового учебного модуля. Определение и приоритизация потребностей в обучении позволит руководителям CPLP сосредоточить свое внимание на вопросах, имеющих наибольшее значение для организации.

Следующие методы могут помочь определить потребности в обучении:

* Определите, какие знания или навыки необходимы в организации, с помощью оценки потребностей в обучении.
* Просматривайте существующие отчеты о работе или анализе заданий.
* Определите любые нормативные или другие требования к программам обучения.
* Анализируйте соответствующие риски кибербезопасности или конфиденциальности для аудитории участников. Все организации сталкиваются с операционными рисками. В то время как большинство соображений о рисках сосредоточены на реагировании на инциденты, которые приводят к неспособности поддерживать кибербезопасность, важно включить эффективный план обучения в качестве фактора снижения рисков.
* Проанализируйте извлеченные уроки или отчеты о принятых мерах. После инцидента руководитель CPLP может быть вовлечен в работу по обучению персонала передовым методам исправления. Это важная возможность учиться на ошибках. Должен быть разработан новый материал, который не только говорит о специфике инцидента, но и может помочь укрепить слабые места вокруг него, такие как выявление уязвимостей и сообщение о них.

# Определите аудиторию программы обучения

На этапе анализа менеджер программы обучения определит и определит аудитории, которые будут обучены целям обучения. Руководителям может быть полезно координировать свои действия с

Функция обучения кибербезопасности и конфиденциальности организации для определения потребности персонала в дополнительном обучении.

Потенциальные аудитории для обучения в рамках CPLP включают:

* **Новые сотрудники:** Эта аудитория включает в себя подрядчиков, и основное внимание обычно уделяется важным политикам и правилам поведения для систем, к которым они будут иметь доступ. Это обучение включает в себя то, что обычно называют «ориентацией новых сотрудников» или «адаптацией», и может быть совместным обучением кибербезопасности и конфиденциальности. В некоторых организациях может потребоваться требовать от посетителей и/или гостей подписания политик допустимого использования, если они разрешают им любой тип доступа к системе, включая использование беспроводных сетевых подключений.
* **Все пользователи:** Это также известно как «общее обучение персонала» и включает в себя регулярное (часто ежегодное, но желательно чащее) обучение кибербезопасности и конфиденциальности для всех пользователей системы, включая персонал, не имеющий доступа к системе. Анализ потребностей этой аудитории в обучении должен включать в себя обзор эффективности предыдущих элементов программы и любых новых организационных требований.
* **Владельцы учетных записей с привилегированным доступом:** это сотрудники с дополнительными обязанностями, которым доверено выполнение функций, связанных с кибербезопасностью или конфиденциальностью, которые обычные пользователи не имеют права выполнять. Им потребуется дополнительное обучение, чтобы получить учетные записи с привилегированным доступом. При определении владельцев учетных записей с привилегированным доступом учитывайте следующее:
  + Внедрены ли новые системы или планируются ли они, а также права и привилегии, связанные с учетными записями с привилегированным доступом
  + Является ли список участников с владельцами системы полным и требуются ли новые права и привилегии
  + Были ли какие-либо из этих систем перенесены в облако и требуют ли они нового обучения
* **Обучение сотрудников со значительными обязанностями в области кибербезопасности и/или неприкосновенности частной жизни:** На некоторых должностях требуется обучение на основе ролей для сотрудников со значительными специализированными обязанностями. Данный вид обучения включает в себя:
  + Специализированное или индивидуальное обучение по конкретным продуктам, сетям, системам, приложениям или информации
  + Задачи и действия рабочих ролей, такие как процедуры реагирования на инциденты, обязанности по надзору или управление идентификацией
  + Программы переподготовки и повышения квалификации
  + Обучение, которое помогает сотруднику выполнять свои рабочие задачи

В следующих примерах показано, как можно распределить персонал по нескольким программам обучения:

* В настоящее время Уилсон является системным администратором, а в качестве сотрудника федерального агентства она посещает ежегодный тренинг CPLP. Она также работает в отделе информационных технологий, поэтому она и ее команда проходят дополнительное обучение по кибербезопасности и конфиденциальности. В своей роли

Как системный администратор, она несет значительную ответственность за кибербезопасность и конфиденциальность, поэтому обязана пройти дополнительное обучение.

* В настоящее время Нг входит в состав команды веб-публикаций организации и имеет права доступа для публикации общедоступных веб-страниц организации. Это накладывает на агентство значительную ответственность за брендинг и коммуникации. Нг должен пройти ежегодное обучение и подписать дополнительную Политику допустимого использования в отношении соответствующей издательской деятельности.

# Сопоставление выявленных потребностей в обучении с каждой аудиторией

Основными знаниями и навыками для сегмента обучающей аудитории «все пользователи» является способность распознавать риски кибербезопасности и конфиденциальности, принимать соответствующие меры для снижения вреда для организации и сообщать о любых инцидентах или событиях, когда это уместно. Все пользователи должны обладать полномочиями и навыками для соблюдения правил поведения организации и политик допустимого использования, которые включают рекомендации по использованию устройств, предоставленных организацией, и доступу к сетевым ресурсам.

Владельцы учетных записей с привилегированным доступом должны иметь возможность правильно оценивать риски и использовать системы, к которым им предоставлен доступ, не создавая дополнительных рисков или вреда для организации. Фреймворк NICE [[5]](#_bookmark106) может быть полезным ресурсом для определения необходимых знаний и навыков на основе ролей для тех, кто несет значительные обязанности в области кибербезопасности или конфиденциальности. Анализ организационной работы также будет полезен для определения целей обучения участников программы. Для тех, кто несет значительные обязанности по защите конфиденциальности, менеджер CPLP должен проконсультироваться с менеджерами, малыми и средними предприятиями и высшим руководством организации по вопросам конфиденциальности (т.е. CPO или SAOP) для получения дополнительных рекомендаций о знаниях и навыках, необходимых для отдельных лиц.[13](#_bookmark63)

Существуют модели оценки задач, необходимых для роли конкретного человека, такие как учет сложности или трудности задачи, ее важности и частоты выполнения задачи. Иногда это называют «моделью DIF» для учета относительной сложности, важности и частоты выполнения задачи. Это может быть полезно для определения знаний и навыков, на которых CPLP должен сосредоточиться при обучении тех, кто несет значительные обязанности в области кибербезопасности или конфиденциальности.

# Оцените текущие знания и уровень навыков аудитории

Следующим шагом на этапе анализа является определение того, что сегмент аудитории уже знает о теме и какими навыками он обладает, держа в голове цель обучения. CPLP должна быть направлена на предоставление учащемуся необходимого объема новых знаний и навыков

13 Публичная рабочая группа NIST Privacy Workforce работает над выявлением и документированием задач, знаний и навыков, которые соответствуют Концепции конфиденциальности NIST. Для [получения дополнительной информации см.](https://www.nist.gov/privacy-framework/workforce-advancement/privacy-workforce-public-working-group)  https://www.nist.gov/privacy-framework/workforce-advancement/privacy-workforce-public-working-group.

при этом закрепляя имеющиеся знания и навыки. Существует несколько методов определения имеющихся знаний и навыков:

* Проводите беседы и интервью с малыми и средними предприятиями, менеджерами, владельцами систем и другими сотрудниками организации, выполняющими соответствующие миссии или бизнес-функции.
* Просмотр последних анализов рабочих задач
* Анализируйте события и связанные с ними реакции, которые могут указывать на уровень мастерства
* Проведение оценки производительности для оценки и проверки возможностей
* Проведение обучения с использованием существующих элементов программы CPLP для определения базовых показателей

Эти методы также позволяют определить, требуется ли новое обучение для роли или необходимо обновить или изменить существующее.

# Определите пробелы в обучении

На данный момент анализ измеряет имеющиеся знания и навыки персонала с обзором каждого сегмента аудитории. Разница между этим и идеальным состоянием знаний и навыков для цели обучения называется «разрывом в обучении». На этапе разработки менеджер CPLP будет использовать информацию о каждом пробеле в обучении (по цели обучения, аудитории обучения и т. д.) для разработки программы, достаточно специфичной для удовлетворения каждой потребности.

# Этап проектирования

В начале этапа проектирования подумайте, какие знания и навыки нужны аудитории для изучения или развития и какие пробелы будет закрыт учебным материалом. Это будет стимулировать постановку целей обучения и процесс их достижения. Процесс разработки должен завершиться составлением систематического плана подхода, необходимого для того, чтобы СПЯС восполнило выявленные пробелы в знаниях и навыках.

# Этапы этапа проектирования

Менеджер CPLP начинает формальную фазу проектирования CPLP или нового элемента в текущей CPLP с создания проектного документа, в котором излагаются требования. Затем необходимо будет определить, нужно ли им создавать или покупать учебные материалы, чтобы удовлетворить эти требования. На этапе проектирования находятся следующие этапы:

1. Создание дизайн-документа
2. Провести обзор доступного обучения, как внутреннего, так и внешнего
3. Определение целей обучения
4. Обобщение CPLP или требований к элементам

# Создание дизайн-документа

Проектная документация представляет собой план разработки и реализации элементов программы обучения. Обычно он создается менеджером CPLP и проверяется ключевыми заинтересованными сторонами (когда это необходимо для финансирования и других согласований) перед переходом к этапу разработки.

Типичные элементы проектного документа включают:

* Цель, задачи и предпосылки
* Целевая аудитория
* Цели обучения
* Содержание и доступный обучающий опрос (например, сборка или покупка)
* План курса, включающий темы высокого уровня (например, количество уроков или модулей и их продолжительность)
* Стратегия обучения, включающая в себя средства массовой информации (например, аудио, видео, демонстрации, имитации, симуляции), упражнения и упражнения.
* Средство доставки (т. е. учебная среда — онлайн, в классе и т. д.)
* Виды оценивания (например, участие, викторина с проходным баллом, оценка навыков на основе результатов и т. д.)
* Обязательные измерения и метрики
* Страница подписи для документального подтверждения принятия от ключевых заинтересованных сторон

Основываясь на своих ресурсах, организация будет определять, может ли она создавать, создавать или использовать существующий правительственный или коммерческий учебный контент (COTS), который обсуждается далее в разделе Разд. [4](#_bookmark72).

# Проведение опроса о доступных учебных курсах

Менеджерам CPLP необходимо будет определить, какие учебные материалы ранее использовались в их организации и до сих пор доступны и пригодны для использования. Кроме того, могут быть материалы и программы, доступные из других подразделений организации, агентства или партнерских агентств. Федеральные ресурсы могут располагать материалами, презентациями и даже докладчиками, доступными для удовлетворения различных целей обучения. Важным результатом исследования будет понимание того, что в настоящее время делается для удовлетворения потребностей в обучении в организации, а также пробелов в необходимых программных материалах. Содержание должно быть адаптируемым в соответствии с потребностями участников программы обучения и организационным контекстом с разумными усилиями или затратами.

# Внешние источники материалов CPLP

Существует множество внешних источников материалов CPLP. Некоторые возможные источники включают:

**Поставщики: Если** организация решает передать часть или всю разработку курсов CPLP на аутсорсинг, ряд поставщиков в частном секторе предлагают курсы COTS, которые подходят для определенной аудитории или могут быть разработаны для конкретной аудитории. Прежде чем выбирать поставщика, агентства должны полностью понимать свои потребности в CPLP, быть в состоянии определить, соответствует ли материал потенциального поставщика этим потребностям, и учитывать, кто «владеет» материалом для целей будущих обновлений и адаптаций. Сотрудник по контрактам агентства поможет обеспечить соблюдение организационных руководящих принципов.

**Некоммерческие организации и соглашения на основе грантов:** Федеральные организации могут заключать соглашения с некоммерческими организациями, гранты университетам или другие подобные договоренности для создания учебных материалов по вопросам кибербезопасности или конфиденциальности. Менеджеры CPLP должны быть осведомлены о любых таких возможностях и использовать эти материалы.

**Другие организации:** Организации могут изучать материалы CPLP, разработанные другими организациями, и редактировать их в соответствии со своими потребностями, а не создавать совершенно новый курс. Следует позаботиться о том, чтобы доступный материал был применим к целевой аудитории и отвечал целям обучения организации.

**Совместные мероприятия и материалы:** Федеральные агентства могут предлагать учебные мероприятия по кибербезопасности и конфиденциальности, открытые для сотрудников правительства. Менеджеры CPLP должны присоединяться к федеральным рабочим группам (например, Federal Information Security Educators или FISSEA[14](#_bookmark68)), чтобы быть в курсе событий, семинаров и конференций, предназначенных для профессионального развития.

Источниками своевременного материала могут быть:

Информационные бюллетени по электронной почте, выпущенные отраслевыми новостными группами, академическими учреждениями или отделом кибербезопасности или конфиденциальности организации

Веб-сайты, посвященные кибербезопасности или конфиденциальности

Тематические мероприятия, такие как Неделя конфиденциальности данных[15](#_bookmark69), Месяц осведомленности о кибербезопасности[16](#_bookmark70) или Неделя карьеры в области кибербезопасности 17

Конференции, семинары, вебинары, форумы и курсы

14 См. [https://www.nist.gov/itl/applied-cybersecurity/fissea.](https://www.nist.gov/itl/applied-cybersecurity/fissea)

15 См. [https://staysafeonline.org/programs/data-privacy-week/.](https://staysafeonline.org/programs/data-privacy-week/)

16 См. [https://staysafeonline.org/programs/cybersecurity-awareness-month/.](https://staysafeonline.org/programs/cybersecurity-awareness-month/)

17 См. [https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-week.](https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-week)

# Внутренние источники материалов CPLP

Менеджеры CPLP могут строить новые партнерские отношения или укреплять существующие с функциональными менеджерами организации, которые координируют или проводят свои собственные программы обучения. Функциональное обучение, разработанное собственными силами (например, финансовые приложения или управление персоналом), часто не содержит адекватного обсуждения связанных с этим вопросов кибербезопасности и конфиденциальности. Благодаря такому межведомственному партнерству менеджеры CPLP могут просматривать существующие ссылки на тематические области в материалах, проверять полноту и точность, а также помогать функциональному руководителю в разработке учебного модуля для любого материала, который ранее не содержал компонента кибербезопасности или конфиденциальности.

# Определение целей обучения: от анализа к проектированию

Менеджеры CPLP обобщают то, что они нашли в доступных материалах, чтобы определить цели обучения для CPLP. Независимо от того, работает ли менеджер CPLP над всем планом, разрабатывает несколько новых элементов или обновляет существующие, этот этап может быть очень полезен для обеспечения тесной увязки усилий с выявленными потребностями организации.

# Примеры определения целей обучения

Рассмотрим следующие примеры выявленных пробелов в обучении и связанных с ними целей обучения.

**Сценарий 1:** Недавний анализ показал, что сотрудники, работающие на местах, удаленно и удаленно, в том числе сотрудники с учетными записями с привилегированным доступом, используют однофакторную аутентификацию (т. е. пароль). Директор по информационным технологиям одобрил внедрение системы токенов многофакторной аутентификации, начиная с учетных записей с привилегированным доступом в первом квартале и всех остальных учетных записей во втором квартале. Менеджеру CPLP было поручено помочь сотрудникам понять их роль в использовании этой новой системы многофакторной аутентификации.

# Фаза анализа: выявление пробелов в знаниях и навыках

Поскольку это новый метод аутентификации, сегменты аудитории «всех пользователей» и владельцев учетных записей с привилегированным доступом нуждаются в информации и обучении по новым политикам, процессам и процедурам доступа к системе. Кроме того, они должны знать, почему эта работа важна или как она защищает информацию и активы в корпоративных системах. Владельцам учетных записей с привилегированным доступом также потребуется дополнительная информация о конкретных привилегиях, которые они получат после аутентификации в системе.

# Этап проектирования: Постановка целей обучения на основе пробелов в знаниях и навыках

Затем должны быть установлены цели и задачи обучения для программы. В этом примере цели и задачи программы обучения включают в себя предоставление сотрудникам:

* Понимание уязвимостей, связанных с использованием однофакторной аутентификации (например, идентификатор пользователя и пароль)
* Узнайте, почему организация внедряет метод маркера многофакторной проверки подлинности
* Определение их роли в использовании многофакторной проверки подлинности
* Установите приложение для проверки подлинности и убедитесь, что маркер получен
* Используйте токен в 100 % случаев для аутентификации в системе

**Сценарий 2:** Недавний внешний аудит политики и практики обеспечения конфиденциальности системы организации показал, что сотрудники финансового отдела не обеспечивали адекватной защиты конфиденциальности банковской информации сотрудников при обработке командировочных расходов сотрудников.

# Фаза анализа: выявление пробелов в знаниях и навыках

На этапе анализа менеджер программы обучения определил, что сотрудники финансового отдела назначены как сотрудники, несущие значительные обязанности в области кибербезопасности и конфиденциальности, и проходят ежегодный часовой курс обучения для самостоятельного изучения. На основе анализа было установлено, что сотрудникам финансового отдела не хватало базового понимания политики и процедур защиты конфиденциальной информации и информации, связанной с неприкосновенностью частной жизни. Поскольку это может иметь немедленные и разрушительные последствия, этот недостаток знаний будет устранен с помощью индивидуального решения для обучения, которое будет предоставлено немедленно и включено в обновленную информацию ежегодного часового учебного курса для самостоятельного изучения.

# Этап проектирования: Постановка целей обучения на основе пробелов в знаниях и навыках

Был запланирован вебинар с сотрудниками финансового отдела, чтобы дать немедленные указания по корректирующим действиям по защите конфиденциальной банковской информации сотрудников. Целями и задачами обучения являются:

* Чтобы иметь возможность описать, что считается конфиденциальной или личной информацией, включая банковскую информацию
* Чтобы иметь возможность описать политики и процедуры защиты конфиденциальной и личной информации
* Чтобы иметь возможность адекватно защищать информацию во время использования и во время ее хранения в системе при наличии онлайн-формы, содержащей информацию, связанную с конфиденциальностью

# Обобщение CPLP или требований к элементам

Прежде чем перейти к этапу разработки, руководитель CPLP должен консолидировать требования к разработке с использованием результатов этапов анализа и проектирования. Должна быть возможность полностью сформулировать пробелы в компетенциях, на которые нацелен сегмент участников программы обучения, и связанные с ними цели обучения.

Также важно учитывать следующие требования CPLP:

* Материал должен учитывать все стили обучения (например, онлайн, лично, повторяемый, записанный) и работать для разных типов и размеров аудитории.
* Элементы программы должны соответствовать стандартам доступности.
* Контент должен обновляться и поддерживаться, чтобы оставаться актуальным.
* Следует признавать и поддерживать многообразие рабочей силы.
* Цели обучения должны быть предусмотрены для любого элемента обучения или учебного материала.
* Цели обучения должны быть установлены в соответствии с миссией организации.
* Каждой цели обучения должен быть посвящен отдельный раздел, а для каждой из целей обучения должны быть созданы индивидуальные уроки.
* Визуальные элементы (например, графика, видео, таблицы и другие визуальные инструменты) должны быть интегрированы для усиления важных концепций.
* Взаимодействие должно вовлекать аудиторию и способствовать ее способности переносить контент из учебной среды на рабочее место.
* Менеджеры и супервайзеры должны иметь возможность проверять ход выполнения, создавать отчеты и получать доступ к LMS.
* Следует поддерживать потребности в обязательной отчетности для исполнительного руководства.
* Сотрудники ИТ-службы и службы технической поддержки должны пройти подготовку для поддержки CPLP.
* Если вы используете курсы на аутсорсинге, поставщики должны иметь поддержку и возможность обновлять платформы отчетности и LMS.

# Разработка и внедрение СПЯС

На этапе разработки требования каждой аудитории оцениваются, бюджетируются и предусматриваются отдельно. Ранее выявленные требования аудитории и цели обучения являются руководящими факторами для разработки контента. Некоторые организации могут иметь существующие и зрелые программы повышения осведомленности, обучения и образования, которые могут предоставить контент или повлиять на этапы разработки и внедрения. При разработке учебного контента следует учитывать сложившуюся передовую практику и извлеченные уроки.

В процессе разработки будет задействован различный персонал, в том числе:

* **Управление:** Все уровни управления будут нести ответственность за потребности своих сотрудников в обучении, определение приоритетности учебных ресурсов, выявление пробелов в обучении и оценку эффективности обучения.
* **Специалисты по кибербезопасности и конфиденциальности и малые и средние предприятия:** Специалисты и малые и средние предприятия помогают определить задачи, знания и требования к навыкам для ролей или должностных функций; выявляют пробелы в обучении и потребности в организации; а также руководят разработкой и анализом учебных материалов.
* **Специалисты по обучению:** Специалисты по обучению приобретают, настраивают, разрабатывают, представляют и оценивают содержание обучения и программы обучения. Независимо от того, работают ли учебная группа и команды по кибербезопасности и конфиденциальности в одном отделе или нет, группы будут тесно сотрудничать с другими малыми и средними предприятиями, чтобы гарантировать, что материалы и программы являются актуальными и точными.
* **Приобретения и бюджет:** Эти отделы будут задействованы, когда обстоятельства и потребности потребуют разработки или приобретения услуг или контента из внешних источников.

После того, как базовые требования программы будут закреплены, может быть разработана и внедрена стратегия обратной связи, чтобы гарантировать, что материалы продолжают поддерживать стратегию CPLP и удовлетворять выявленные потребности в обучении.

# Разработка материалов CPLP

После того как менеджеры CPLP завершат анализ и проверку проекта, они получат в свое распоряжение полный набор проектной документации для руководства разработкой новых материалов. Эти документы полезны при распределении бюджетов и персонала для создания новых материалов или элементов программы. Тем не менее, потребуется дополнительная информация, чтобы направлять создателей контента в их работе.

# Общие руководящие принципы разработки или приобретения новых материалов CPLP

Менеджеру CPLP потребуется создать документ с требованиями, если необходимо создать или найти новое содержание CPLP, учебные планы или другие элементы программы. Документ с требованиями включает в себя информацию из проектной документации, а также любую дополнительную и необходимую информацию, которую необходимо предоставить разработчикам, редакторам и дизайнерам обучения и учебных программ, будь то

Они являются штатными или поставщиками. Документ с требованиями также будет полезен для функций организации по закупкам и бюджету.

Документ с требованиями обычно содержит подробные и конкретные критерии, связанные с содержанием, необходимым для достижения целей обучения. Типичные подсказки или вопросы, которые следует рассмотреть при создании документа с требованиями к любому новому материалу CPLP, включают:

* Для каких сегментов аудитории программы обучения предназначен новый элемент?[18](#_bookmark75)
* Какие конкретные риски и поведение в области кибербезопасности или конфиденциальности стремится устранить организация?
* Какие знания или навыки должен приобрести или усовершенствовать учащийся в результате использования элемента CPLP?
* Способствует ли материал формированию позитивной культуры кибербезопасности и конфиденциальности, которая усиливает роль всех пользователей в снижении организационных рисков?
* Будет ли задействован персонал?
* Каковы бюджетные требования, ограничения и сроки?
* Кто в организации будет проверять разработку и утверждение контента?
* Какое пользовательское тестирование будет проводиться для того, чтобы убедиться, что контент подходит для сегмента участников программы обучения, отвечает их потребностям и уровню навыков?
* Были ли включены измерения и метрики, чтобы гарантировать, что учебная программа предоставит необходимые данные для улучшения следующей версии контента?

Критерии программы обучения для документа с требованиями могут включать следующие соображения:

* Контент должен быть актуальным, актуальным и не устаревать быстро.
* Контент предоставляется в форматах, которые поддерживают офисных и удаленных сотрудников, подрядчиков и гостей.
* Контент доставляется в форматах, подходящих для тех, кто использует адаптивные технологии (например, программы чтения с экрана).
* Учебные материалы включают в себя качественные и количественные оценки и оценки для измерения целей и результатов обучения и приводятся в соответствие с определенными измерениями и показателями.
* Учебный материал специфичен для сегментов участников программы обучения (т.е. аудитории), для которых он предназначен.

18 См. [2.5](#_bookmark39) Для проверки того, кто входит в сегменты аудитории Программы обучения «Все пользователи», «Владельцы учетных записей с привилегированным доступом» и «Важные обязанности в области кибербезопасности и/или конфиденциальности».

# Разработка новых материалов для программы обучения «Все пользователи»

Элементы программы обучения «для всех пользователей» (см. разд. [2.5.1](#_bookmark41)) поставляются в течение всего года. Тем не менее, могут быть необходимые обновления и итерации контента в зависимости от событий и организационных требований. Убедитесь, что бюджет выделен на обновление контента или внесение изменений в материалы с помощью других методов доставки (например, с помощью видеообучения), если внесение фактических изменений в контент является непомерно дорогостоящим.

Разработка динамичной и эффективной программы обучения для всех пользователей — в частности, презентации кибербезопасности и конфиденциальности — является сложной задачей, особенно когда учащиеся приходят с ожиданием, что им нужно сделать только минимум, чтобы выполнить свои требования к обучению.

Однако, учитывая постоянно меняющийся характер рисков кибербезопасности и конфиденциальности, почти всегда будет новый и важный контент для их понимания.

Подумайте о том, как ключевые идеи будут подкрепляться на протяжении всей программы обучения «для всех пользователей». При необходимости могут быть отправлены освежающие сообщения, чтобы закрепить изменение в поведении. Например, если результаты фишинговой кампании показывают более высокий, чем обычно, рейтинг кликов, может потребоваться повторить кампанию с использованием других средств, чтобы аудитория знала об ожидаемом поведении в системе. Повторяющиеся сообщения становятся сохраненными сообщениями. Используйте материалы программы повышения осведомленности, чтобы программа обучения «для всех пользователей» оставалась актуальной, не становясь монотонной или навязчивой. Это сложный баланс, требующий различных форматов доставки и сообщений. Рассмотрите возможность варьирования методов программы повышения осведомленности, таких как ежемесячная рассылка электронных писем на тему кибербезопасности или конфиденциальности, добавление сообщения кампании в официальный блок подписи каждой организации в рамках Месяца осведомленности о кибербезопасности в октябре или Недели конфиденциальности данных в январе или размещение плакатов в столовой агентства круглый год.

Выбор методов распространения сообщений о кибербезопасности и конфиденциальности в организации зависит от доступных ресурсов и сложности сообщений. Некоторые методы, которые подходят для одного сообщения, включают плакаты, скринсейверы, предупреждающие баннеры, общеорганизационные электронные письма, семинары и программы награждения. К методам, которые могут легко включать несколько сообщений или тем, относятся списки «что можно и чего не делать», информационные бюллетени по электронной почте, веб-сеансы, сеансы телеконференций, личные сеансы под руководством инструктора и обмен подписями по электронной почте. Примеры информационных материалов можно посмотреть на веб-сайте Федеральной организации преподавателей информационной безопасности (FISSEA) 19 в разделе «Конкурс FISSEA по повышению осведомленности и обучению в области безопасности».

Дополнительные соображения при разработке программы обучения для всех пользователей включают:

* О чем организация хочет, чтобы все сотрудники знали в отношении кибербезопасности и конфиденциальности? Отправные точки могут включать в себя обзор последних основных рисков для организации, о которых сообщает отдел кибербезопасности или конфиденциальности; общие риски, о которых сообщают организации по кибербезопасности и конфиденциальности; и новые цели миссии, связанные с кибербезопасностью или конфиденциальностью. Оценка организационной политики, обзоры программ, внутренние аудиты,

19 См. [https://www.nist.gov/itl/applied-cybersecurity/fissea.](https://www.nist.gov/itl/applied-cybersecurity/fissea)

Самооценка и выборочные проверки также могут помочь менеджерам программ обучения определить дополнительные темы для рассмотрения.

* Были ли обнаружены ограничения на этапе анализа? Например, есть ли у организации особые проблемы с предоставлением персоналу программы обучения? Сможет ли персонал получить доступ к обучению или пройти его к определенной требуемой дате, чтобы завершить его? Работает ли какой-то персонал удаленно, путешествует, находится за границей или нуждается в разумных условиях? Подумайте, какие дополнительные шаги потребуются для обеспечения того, чтобы весь персонал мог участвовать в программе обучения «все пользователи» и выполнять свои обязательства по программе обучения.
* Популярными темами учебных программ для данного сегмента участников могут быть: эксплойты социальной инженерии (например, фишинг, целевой фишинг, вишинг, смишинг); политика паролей и управление ими; многофакторная аутентификация; изменение паролей по умолчанию (например, на маршрутизаторах и устройствах IoT); соображения кибербезопасности и конфиденциальности при удаленной и удаленной работе из дома; кибербезопасность во время путешествий; безопасность электронной почты; вредоносные программы, в том числе программы-вымогатели и способы реагирования; плечевой серфинг и соображения об инсайдерских угрозах; резервная политика и управление; облачные сервисы; а также политики утилизации компьютеров, телефонов и данных.

# Разработка новых материалов для Программы обучения владельцев учетных записей с привилегированным доступом

Разработка новых материалов или элементов для владельцев учетных записей с привилегированным доступом аналогична их разработке для сегмента «все пользователи». Создайте документ с требованиями, который сопоставляет цели обучения для этого сегмента аудитории с доступным финансированием и организационными требованиями.

Дополнительные соображения по разработке новых материалов для программы обучения владельцев учетных записей с привилегированным доступом включают:

* О чем следует знать владельцам учетных записей с привилегированным доступом в отношении кибербезопасности и конфиденциальности?
* Какие процедуры необходимо соблюдать персоналу для защиты своих учетных записей с привилегированным доступом?

Некоторые отправные точки включают в себя: понимание прав и привилегий, предоставленных этому сегменту аудитории программы обучения; анализ рисков, связанных с учетными записями с привилегированным доступом или системами или приложениями, связанными с привилегированным доступом; рассмотрение этих вопросов с офисами CIO, CISO и/или CPO; и согласование целей обучения по этим рискам с имеющимся бюджетом для затронутого персонала и отделов. Оценка организационной политики, обзоры программ, внутренние аудиты, самооценки и выборочные проверки также могут помочь менеджерам CPLP определить дополнительные темы для рассмотрения.

# Разработка новых материалов для тех, кто несет значительную ответственность за кибербезопасность и/или неприкосновенность частной жизни

Индивидуальный и индивидуализированный характер непрерывного развития навыков и обучения персонала со значительными обязанностями в области кибербезопасности и/или конфиденциальности требует более детального и детального подхода к программе обучения. Например, может потребоваться несколько документов с требованиями для разработки новых элементов программы обучения и определения обучения, которые будут удовлетворять целям обучения. Менеджер CPLP должен сотрудничать и координировать эти усилия с отделом человеческого капитала организации, CLO, разработчиками тренингов и учебных программ, а также с отдельными менеджерами и руководителями персонала в этом сегменте аудитории учебной программы.

Руководители CPLP должны обеспечить, чтобы сложность обучения была соизмерима с ролью и потребностями людей, которые будут проходить обучение. Учебные материалы по кибербезопасности и конфиденциальности на основе ролей могут быть разработаны на начальном уровне для человека, который только изучает дисциплину. Материалы могут быть разработаны на среднем уровне для того, кто имеет больше опыта и, следовательно, больше ответственности на своем рабочем месте. Передовые материалы могут быть разработаны для малых и средних предприятий, чья работа включает в себя высочайший уровень доверия и сопутствующий высокий уровень ответственности в области кибербезопасности или конфиденциальности.

# Получение учебных материалов из внешних источников

Менеджеры CPLP должны оценивать доступные материалы из различных внешних источников, включая федеральные программы и репозитории, отраслевых поставщиков и академические учреждения. Некоторые из этих курсов или элементов обучения могут быть недорогими или даже бесплатными.

Если позволяет бюджет, менеджеры CPLP могут приобрести (или лицензировать) библиотеку курсов, предоставленную поставщиком, и согласовать, курировать и рекомендовать набор этих курсов для аудитории учебной программы или определенных рабочих ролей. При приобретении материалов CPLP следует руководствоваться теми же критериями обучения, которые были определены для создания новых элементов (см.. [3.3.1](#_bookmark67)). Менеджеры CPLP также должны проконсультироваться с агентским бюро по контрактам своей организации.

# Проведение тестирования учащихся на новых элементах CPLP

Включите этап тестирования учащегося («пользовательское тестирование») для всех новых элементов CPLP до их внедрения. Контент должен оцениваться для каждого сегмента аудитории программы обучения, чтобы убедиться, что он соответствует их потребностям и уровню навыков. Дополнительное тестирование учащегося может включать оценку метода доставки предполагаемого элемента, пригодности языка, ценности для учащегося и общего принятия нового элемента. Обратная связь от тестирования учащихся должна быть итеративной и учитываться на каждом этапе проектирования, а не только в форме оценок после внедрения.

# Внедрение новых элементов CPLP

Под реализацией понимается фактическое распространение и доставка материалов CPLP. На этом этапе основное внимание уделяется связи между учащимся и содержанием. Как только план на

Осуществление CPLP было доведено до сведения руководства и принято им (см. разд. [2.11](#_bookmark57)), можно приступать к этапу внедрения. Используйте процесс жизненного цикла при реализации программы, чтобы избежать сценария «один раз и готово», и периодически проверяйте программу на предмет обновлений и исправлений.

# Шаги по реализации нового элемента CPLP

Менеджеры CPLP должны внедрить новую программу обучения или отдельный элемент с теми же повторяющимися шагами. Крайне важно, чтобы все участники этапа реализации были вовлечены в хорошо продуманную коммуникационную деятельность. Это гарантирует, что персонал и его менеджеры или руководители хорошо информированы о любых предстоящих возможностях CPLP, которые имеют отношение к их требуемым планам обучения. Фаза внедрения также является временем для подтверждения того, что требуемая отчетность и метрики могут быть удовлетворены на последующих этапах программы. Шаги, которые следует рассмотреть перед началом этапа внедрения, включают:

1. Информирование о ходе осуществления CPLP
2. Измерение успеха путем установления требований к измерениям, показателям и отчетности
3. Построение графика CPLP
4. Планирование оценки успешности программы путем анализа отзывов, измерений и показателей после внедрения

# Информирование о ходе осуществления CPLP

Коммуникация является важной частью развития общей культуры организации по поддержке усилий по программе обучения. Менеджеры CPLP должны разработать план коммуникаций для каждого этапа реализации элемента программы и включить в него команду по связям с общественностью организации. Менеджеры CPLP также должны определить подходящее время для информирования менеджеров, руководителей и, возможно, задействованного персонала о предстоящих и необходимых элементах программы обучения, а также частоту рассылки напоминаний и других форм коммуникации, способствующих сотрудничеству со стороны организации.

Каждый отдельный элемент CPLP (например, презентация, курс или настольное упражнение) требует отдельной и более подробной формы коммуникации для информирования учащихся и их руководителей о важных деталях учебного мероприятия. Это включает в себя такие элементы, как:

* Названия, описания, цель тренинга или учебной деятельности (включая предварительные условия), цели обучения, задачи и результаты обучения
* Сегменты аудитории, участвующие в программе обучения (если не все пользователи)
* Метод отслеживания (и отслеживания завершения), включая последствия незавершения обучения, особенно для контента в произвольном темпе (к дедлайну или вообще)
* Способ проведения (например, лично, виртуально, самостоятельное онлайн-обучение и т. д.)
* Обязательные, рекомендуемые или запрашиваемые приспособления
* Рекомендации по планированию, такие как сроки регистрации, даты доступности или сроки выполнения
* Проверка учащихся со значительными обязанностями в области кибербезопасности или конфиденциальности

Коммуникационный план должен включать четкое объяснение того, почему программа обучения является обязательной (если применимо) и преимущества участия в ней (т.е. результаты обучения). Следует ссылаться на применимое федеральное законодательство, нормативные акты и политику агентства или организации.

Каждая аудитория учащихся должна быть указана для назначенного обучения. Например, если в политике организации указано, что все пользователи системы должны пройти определенное обучение для получения или поддержания доступа к корпоративным системам, план коммуникаций должен включать это уведомление. Для тех, кто несет серьезные обязанности в области кибербезопасности или конфиденциальности, определите, какое обучение назначено для конкретной рабочей роли, человека или отдела.

Сотрудники должны знать о последствиях невыполнения учебной деятельности в соответствии с политикой организации. Это должно быть объяснено в плане коммуникаций программы обучения и отмечено в описании курса в плане обучения в LMS.

Другие соображения в отношении коммуникаций CPLP включают:

* Названия и номера курсов должны быть уникальными, дифференцированными и включать информацию о способе доступа (например, онлайн или лично), доступности, датах и сроках проведения курсов.
* Все учащиеся, их менеджеры или руководители, а также отделы управления человеческим капиталом должны быть проинформированы обо всех необходимых тренингах и связанных с ними сроках выполнения. Коммуникация должна включать в себя напоминания, ссылки и ссылки на официальные заявления о политике организации в отношении информационных систем для сотрудников, а также о последствиях невыполнения учебной деятельности.

# Установление измерений, метрик и отчетности

Как отмечается в. [2.4](#_bookmark35). Менеджеры CPLP должны стремиться к тому, чтобы внедрение всех новых элементов CPLP (например, курсы, тренинги, плакаты, практические упражнения и т.д.) позволило установить и собрать показатели эффективности и измерения. Проанализируйте эти требования на этапе разработки, чтобы убедиться, что измерения по-прежнему соответствуют ожиданиям, таким как нормативные требования и требования к годовой отчетности, цели обучения и результаты обучения. Цель состоит не только в том, чтобы соответствовать требованиям, но и в том, чтобы обеспечить непрерывную работу по разработке CPLP. Как уже упоминалось в. [3.2.2,](#_bookmark66) измерения и метрики включены в требования к дизайн-плану, используемые разработчиками учебных программ и контента.

Вот некоторые рекомендации по отчетам об измерениях и метриках:

* Интеграция LMS: любая используемая автоматизированная LMS должна обеспечивать возможность отслеживания всех необходимых мер, таких как регистрация, посещаемость и завершение обучения.
* Интегрированные элементы, не относящиеся к LMS: Подумайте о том, как будет отслеживаться и регистрироваться участие и успеваемость каждого учащегося, если обучение является очным, виртуальным или гибридным (например, ручное или бумажное отслеживание).
* Рассмотрите показатели того, как элемент CPLP способствует положительной культуре кибербезопасности и конфиденциальности, а также улучшает поведение.

В качестве заключительного шага руководитель CPLP встретится с Комитетом высшего руководства, чтобы проанализировать эффективность программы, рассмотреть новые организационные риски или проблемы, которые следует включить в содержание учебной программы, и определить любые области, требующие значительного улучшения. В разделе [5](#_bookmark89) представлена дополнительная информация о том, как измерения и метрики помогают гарантировать, что жизненный цикл CPLP является непрерывной и непрерывной работой.

# Построение графика CPLP

Создание основного календаря для действий CPLP, который может быть автоматизирован с помощью LMS. Обеспечьте доступ в масштабах всей организации, чтобы сотрудники могли найти элементы, применимые к каждому сегменту аудитории (например, по дате, цели обучения и т. д.). Согласуйте этот календарь с доступностью организации, например с отмечаемыми праздниками, запланированными событиями, крупными ИТ-релизами и другими соображениями, которые могут вызвать конфликты учащихся с расписанием CPLP. В рамках плана коммуникаций разошлите напоминания, чтобы убедиться, что инструкторы и материалы определены и распределены заблаговременно.

# Планирование для оценки успешности программы

После того, как какой-либо элемент CPLP был поставлен или внедрен, менеджер CPLP должен начать действия после внедрения, которые стимулируют оценку и улучшения.[20](#_bookmark88) Некоторые элементы осведомленности, такие как измерение вовлеченности участников программы обучения, могут быть затруднены, особенно в отношении пассивных элементов, таких как плакаты или подписи к электронным письмам. Тем не менее, измерить воздействие можно. Один из методов может включать в себя опрос выборки учащихся, чтобы обсудить их знакомство с сообщениями или то, применяли ли они какие-либо советы.

Некоторые ключевые моменты, которые следует учитывать на этапе реализации:

* Отправка опросов после обучения
* Проведение опросов для обратной связи с преподавателями
* Определение показателей посещаемости и завершения обучения по учащимся или факультетам
* Другая обязательная или организационная отчетность
* Согласование бюджета
* Консолидация всех опросов обратной связи, метрик и других отчетов CPLP для подготовки материалов для оценки и улучшения

20 В разделе [5](#_bookmark89) обсуждается, как оценить успешность программы путем распространения, сбора, анализа и составления отчетности о результатах работы CPLP с использованием всех доступных отзывов, измерений и показателей после внедрения (см. разд. [2.4)](#_bookmark35) и элементы учебной программы (см. разд. [пункт 4.4](#_bookmark85)).

# Оценка и совершенствование CPLP

Эффективная CPLP удовлетворяет потребности учащихся и организации путем измерения и оценки эффективности программы на постоянной основе. Этот процесс требует современных знаний, осведомленности и понимания законодательных и нормативных требований к организации, а также рисков кибербезопасности и конфиденциальности. Менеджеры CPLP работают с руководителями организаций, учебным персоналом и учащимися для обмена отчетами о результатах деятельности и принятием решений на всех этапах CPLP. Анализ организационных рисков (например, уменьшение количества и частоты распространенных проблем, на решение которых нацелена программа обучения с течением времени) и анализ эффективности материалов (например, отзывы учащихся о курсах) важны для постоянного совершенствования CPLP в условиях меняющегося ландшафта угроз. Не забывайте выбирать измерения, которые можно измерить количественно, например цели SMART (т. е. конкретные, измеримые, достижимые, релевантные и ограниченные по времени).

# Шаги по оценке и совершенствованию CPLP

Процесс оценки и совершенствования CPLP может варьироваться в зависимости от организации и имеющихся ресурсов. Рассмотрите следующие шаги в рамках оценки эффективности CPLP, будь то для всего CPLP, для каждого сегмента аудитории или для отдельного элемента CPLP.

* Создайте отчет об оценке CPLP:
  + Анализируйте измерения и метрики.
  + Проверяйте соответствие нормативным требованиям и отчетность.
  + Оценка эффективности CPLP с помощью обратной связи.
* Ознакомьтесь с отчетом об оценке CPLP вместе с высшим руководством:
  + Договориться об изменениях, которые необходимо внести в CPLP.
  + Оценка бюджетных требований для улучшения программы.
* Приложите усилия для улучшения CPLP:
  + Пересмотр и обновление стратегических и оперативных планов СПЯС.
  + Вносите изменения в следующие редакции элементов программы и графика.

# Создание отчета об оценке CPLP

В конце кампании и регулярно в течение года по согласованию с Комитетом высшего руководства, менеджеры CPLP должны подготовить итоговый документ для рассмотрения со старшим руководством. В этом отчете будет представлен анализ посещаемости, отзывов, измерений и других показателей, а также помогут определить действия, области для улучшения и следующие шаги. Он должен быть адаптирован для высшего руководства с использованием соответствующего языка и формулировок (например, избегать использования технического жаргона без объяснений).

Отчет об оценке CPLP включает:

* Измерения и метрики (разд. [5.2.1](#_bookmark92))
* Информация о соответствии нормативным требованиям (разд. [5.2.2)](#_bookmark93)
* Оценка эффективности CPLP (разд. [5.2.3](#_bookmark94))
  + Оценка инструктора (разд. [5.2.3.1](#_bookmark95))
  + Оценка содержания (разд. [5.2.3.2](#_bookmark96))
  + Обратная связь с учащимися, руководителями и организациями (разд. [5.2.3.3](#_bookmark97))

# Измерения и метрики

Измерения и метрики являются ключевыми факторами для оценки и улучшения жизненного цикла CPLP. Процесс разработки и внедрения измерений CPLP требует тщательного рассмотрения и должен определяться целями и задачами программы, а также любыми нормативными требованиями.

То, как организация определяет и собирает свои измерения, приведет к определению и анализу ее показателей. Метрики контролируют достижение целей и задач программы путем количественной оценки уровня внедрения, эффективности и результативности программы при одновременном выявлении возможных улучшений. Эффективный набор показателей может помочь улучшить качество контента и вовлеченность учащихся, получить поддержку от организации, увеличить финансирование, выявить влияние на программу управления рисками кибербезопасности и конфиденциальности, а также продемонстрировать отдачу от инвестиций. Включайте результаты как количественных, так и качественных измерительных приборов.

# Отчетность о соответствии нормативным требованиям

Менеджеры CPLP должны быть осведомлены и готовы участвовать во всех нормативных актах организации, связанных с CPLP, включая требования к отчетности. В некоторых организациях отчетность о соответствии может обрабатываться назначенным отдельным лицом или группой. Для тех организаций, в которых обязанности разделены, крайне важно поддерживать совместную коммуникацию, чтобы обеспечить соответствие программы требованиям.

Полностью разработанная и интегрированная CPLP может стать полезным инструментом для поддержки управления рисками предприятия, хотя многие из них изначально разрабатываются для удовлетворения требований законодательства, нормативных актов, политик или стандартов. Выполнение этих обязательств по соблюдению нормативных требований часто является основной задачей руководства более высокого уровня, но должно быть только отправной точкой для надежной программы CPLP. Примерами общих количественных показателей, демонстрирующих соответствие CPLP, являются обучение определенного процента рабочей силы и результаты практических занятий.

Организации должны определить, каких показателей соответствия они должны достичь, и учесть эти исходные данные при разработке CPLP.

Менеджеры CPLP должны работать с владельцами политик, чтобы определить методы, которые CPLP будет использовать для удовлетворения потребностей в отчетности и обеспечения того, чтобы результаты обучения соответствовали требованиям соответствия. Примеры вопросов, которые следует задать, чтобы помочь определить эти потребности, включают:

* Какой персонал получил (или участвовал) в учебном элементе?
* Насколько уровень участия соответствует цели охвата сегмента участников программы обучения?
* Как далеко следует зайти СПЯС в погоне за ожидаемым охватом?
* Выполнили ли сотрудники, занимающие должности, определенные в соответствии с нормативными требованиями, свои требования к обучению?

# Оценка эффективности CPLP

Менеджеры CPLP должны периодически оценивать общую эффективность CPLP и докладывать о результатах руководству, чтобы стимулировать дальнейшую поддержку программы. На этом этапе жизненного цикла программы осуществляется применение метрик и измерений (см.. [2.4](#_bookmark35)) должны быть документально подтверждены.

Помимо обеспечения соответствия нормативным требованиям, сама программа должна уметь достигать собственных целей. Двумя основными компонентами программы для измерения и оценки являются инструкторы и содержание. Менеджеры CPLP должны анализировать работу преподавателей, чтобы убедиться в том, что материал преподается эффективно. Успех контента может быть определен путем учета обратной связи от преподавателей, студентов и руководства. В следующих подразделах описываются потребности в измерениях и метриках для оценки и анализа.

# Оценка инструктора

Инструктор несет ответственность за создание среды, в которой может происходить обучение, путем проведения дискуссий, предоставления знаний и опыта, а также мотивации и вдохновения участников на приобретение новых навыков. Оценка инструктора включает в себя как оценку инструктора, так и обратную связь на основе того, что инструктор наблюдал или испытал.

Менеджеры CPLP и Комитет высшего руководства работают вместе, чтобы найти подходящих инструкторов для своего персонала и достижения целей обучения CPLP, определяя, могут ли организационные ресурсы поддерживать специальную внутреннюю команду инструкторов или необходимы внешние ресурсы для внедрения учебного контента под руководством инструктора. В некоторых организациях менеджер программы обучения кибербезопасности также является менеджером программы обучения по вопросам конфиденциальности и ведущим инструктором.

Поскольку преподаватели являются ключевым фактором в создании благоприятной и эффективной учебной среды, важно контролировать работу преподавателей с помощью наблюдений и других форм обратной связи. Некоторые эффективные качества преподавателя включают в себя то, насколько хорошо преподаватель доносит материал и ключевые концепции до аудитории, взаимодействует с учащимися в позитивной и уважительной манере, поощряет активное участие, использует интерактивные методы обучения и отвечает на вопросы и опасения учащихся.

Обратная связь от преподавателя может быть получена из отзывов слушателя о курсе, а также из прямых ежегодных наблюдений преподавателя. Вот некоторые советы по предоставлению обратной связи учащимся:

* + - * + Предоставьте учащимся возможность оставлять анонимные отзывы, чтобы стимулировать конструктивные отзывы.
        + Задайте учащимся конкретные вопросы о методах преподавания преподавателя, знании предмета и управлении классом.
        + Предоставьте отзыв преподавателю в краткой форме, чтобы случайно не идентифицировать отдельных людей.

Вот некоторые советы по наблюдениям инструктора:

* + - * + Включайте непосредственные наблюдения за преподавателями с помощью опытных разработчиков учебных курсов или супервайзеров, которые могут дать представление о стилях преподавания, управлении классом и взаимодействии с учащимися.
        + Учитывайте замечания других преподавателей в качестве неформального механизма обратной связи.
        + Сообщите инструкторам, когда наблюдатели будут там, и дайте им подготовиться.

Важно создать справедливый и поддерживающий процесс оценки преподавателя, чтобы гарантировать достижение целей обучения и постоянное совершенствование. Сочетание нескольких методов оценки и прозрачного процесса обеспечивает прочную основу для конструктивной оценки. Самое главное, что преподаватели будут знать, что их ценят за их важную роль в программе обучения.

# Оценка контента

Преподаватели также предоставляют важную обратную связь об учебном материале и о том, как он был воспринят учащимися. Менеджеры CPLP должны работать с преподавателями, чтобы проанализировать их комментарии и замечания и, при необходимости, поддержать корректировку материала для большей эффективности. Преподаватели могут оставлять отзывы по следующим вопросам:

* + - * + Воспринимаемая точность
        + Простота обучения и понимание учащимся
        + Адекватность материалов для поддержки контента
        + Актуальность и своевременность материалов

# Оценка и обратная связь со стороны учащихся, руководителей и организаций

Учет различных типов обратной связи может помочь менеджерам CPLP получить полное понимание того, что работает и что необходимо улучшить в CPLP. Механизмы обратной связи могут быть использованы для оценки реакций, знаний, поведения и результатов учащихся — четырех уровней воздействия учащихся в модели Киркпатрика [[15]](#_bookmark116), как показано в таблице 3.

**Таблица 3. Четыре уровня модели Киркпатрика для оценки обучения**

|  |  |  |
| --- | --- | --- |
| **Уровень** | **Удар** | **Описание** |
| Уровень 1 | Реакция | Получите обратную связь от участников о полезности, вовлеченности и атмосфере учебной программы (например, способствующей обучению и т. д.) во время и в конце учебного элемента. |
| Уровень 2 | Учение | Оценивайте участников, чтобы определить, являются ли предполагаемые знания или навыки  были приобретены во время и в конце учебного элемента. |
| Уровень 3 | Поведение | Получите обратную связь от учащихся, коллег и/или руководителей, чтобы определить, применяли ли учащиеся учебные материалы и приобретали ли навыки при выполнении своих рабочих обязанностей. |
| Уровень 4 | Результаты | Получение обратной связи от высшего руководства, чтобы определить, является ли обучение  Результаты – это достижение целей организации. |

Уровень 1 иногда называют «листом улыбки», потому что простая анкета с визуальными подсказками для оценок может быть использована, чтобы спросить учащегося о его непосредственных мыслях о программе обучения. Результаты реакций Уровня 1 могут быть использованы для оценки непосредственного воздействия элемента программы обучения.

На измерения реакции уровня 1 влияют:

* + - * + Общий воспринимаемый уровень вовлеченности и эффективности программы обучения
        + Использование интерактивных механизмов на протяжении всего обучения, таких как вопросы для опросов, интерактивные обсуждения, а также индивидуальные занятия или занятия в небольших группах
        + Использование вопросов опроса в конце курса или других типов сеансов подведения итогов для оценки удовлетворенности учащихся и их восприятия элемента обучения и программы обучения. Примеры вопросов, которые следует задать в конце элемента программы обучения:

Был ли элемент программы обучения актуален для вашей рабочей роли?

Насколько вы удовлетворены контентом, механизмом доставки (например, онлайн-платформой, помещением или инструктором), уровнем вовлеченности, продолжительностью и глубиной материала?

Стоил ли элемент учебной программы вашего времени?

Какие три самые важные вещи вы узнали из элемента учебной программы?

Какая дополнительная информация или другие темы были бы вам полезны?

Каково ваше общее впечатление от программы обучения?

Уровень 2 оценивает, насколько хорошо участник усвоил содержание обучения и приобрел новые знания на основе результатов обучения, которые изложены в формате, который можно измерить, достичь и который основан на результатах. Одним из наиболее распространенных методов измерения успеваемости учащихся является оценка в конце курса, хотя существуют и другие инновационные и увлекательные методы, которые следует рассмотреть и использовать.

Рекомендации по обучению уровня 2 включают:

* + - * + Письменные вопросы или практические задания разработаны на уровне, соизмеримом как со сложностью материала, так и с уровнем понимания, ожидаемым от учащегося
        + Четкие цели обучения и результаты обучения, а также оценки, соответствующие целям и содержанию обучения
        + Практические оценки, которые позволяют продемонстрировать развитие знаний и навыков и которые имитируют то, что вы испытаете в своей рабочей роли.
        + Использование различных методов оценки, таких как тематические исследования, интерактивные виртуальные киберлаборатории, демонстрации и упражнения на основе сценариев

Уровень 3 учитывает, смог ли учащийся применить новые знания или навыки в своих рабочих обязанностях и обязанностях. Получение обратной связи во многом зависит от того, задают ли вопросы учащимся, их сверстникам или руководителю.

Рекомендации по поведению на уровне 3 включают:

* + - * + Вопросы, которые помогают выявить пробелы в материалах учебной программы и могут указывать на необходимость закрепления этих материалов
        + Вопросы, которые помогают выявить пробелы в организационной структуре, ограничивающие способность учащегося применять новые знания и навыки
        + Примеры вопросов для учащихся могут включать:

Как вы использовали знания, полученные в ходе учебной программы, на рабочем месте? Как изменился ваш подход к [трудовой деятельности] после участия в программе обучения? Опишите ситуацию на работе, в которой вы смогли применить свои новые знания или навыки.

Какая дополнительная поддержка учебного контента, подкрепление или вспомогательное пособие помогут вам использовать новые знания и навыки на рабочем месте?

Была ли деятельность лаборатории кибербезопасности по устранению неполадок с несанкционированными IP-адресами достаточной, чтобы помочь вам выполнить эту работу на рабочем месте? Каким образом, если таковое имеется, упражнение в малых группах по определению ролей и обязанностей было полезно для вашего рабочего места?

* + - * + Примеры вопросов для коллег или руководителей могут включать:

Каким образом, если таковые имеются, вы наблюдали или замечали изменения в [трудовой деятельности] учащегося с тех пор, как он принял участие в учебной программе? Наблюдали ли вы, как учащийся делится своими новыми знаниями или навыками с другими?

Какие новые процессы или процедуры необходимо включить в учебные материалы, если таковые имеются? Какие новые направления деятельности или изменения на рабочем месте, если таковые имеются, необходимо включить в учебные материалы?

Как вспомогательные материалы, информационные материалы или помощь в обучении могут помочь закрепить новые знания или навыки?

* + - * + Дополнительные вопросы обычно задаются через три-шесть месяцев после учебного мероприятия, чтобы прошло достаточно времени, чтобы учащийся мог интегрировать учебный материал в свои рабочие обязанности и обязанности.

Обратная связь 4-го уровня определяет влияние, которое программа обучения оказала на организацию, иногда называемое окупаемостью инвестиций (ROI). Менеджеры CPLP анализируют результаты своей деятельности с точки зрения всего предприятия. Например, организация может принять решение о внедрении новой технологии, такой как искусственный интеллект (ИИ), в свои бизнес-процессы.

Обучение содержит политики и процедуры использования учащимся технологий ИИ в своей рабочей роли. Программа требует, чтобы учащиеся посещали обучение, но также требует одобрения руководителя и обоснования его использования. Затем организация должна определить, дали ли результаты обучение по политикам и процедурам или надзорному контролю. Чтобы правильно использовать этот метод оценки, необходимо четко определить требования, цели, общие результаты и показатели.

Цели обучения и результаты обучения должны быть согласованы со стратегическими и деловыми целями и задачами организации в процессе проектирования. Организационная цель, согласованная с целями обучения, должна быть количественно измеримой и детализированной (например, цели «SMART»). Примером согласования организационной цели, целей обучения, результатов учащихся и организационных результатов является:

* + - * + **Организационная цель:** Получив уведомление, сотрудники смогут устранить все известные уязвимости в течение 48 часов после выполнения организационных процессов.

Показателем для определения того, достигнута ли цель организации, является анализ тенденций времени, необходимого персоналу для устранения известных уязвимостей. Установите базовый уровень перед программой обучения и отслеживайте изменения после программы обучения.

* + - * + **Цели обучения:** Участники могут отслеживать известные используемые уязвимости, выявлять последствия для организации, анализировать и документировать индикаторы компрометации, уведомлять заинтересованные стороны, а также реализовывать и документировать стратегии смягчения последствий.
        + **Результаты обучения:** Столкнувшись с известной уязвимостью, учащиеся смогут анализировать воздействие на организацию, находить и документировать индикаторы компрометации, а также реализовывать и документировать мероприятия по смягчению последствий в течение 48 часов.
        + **Организационные результаты:** Менеджер CPLP делится результатами анализа тенденций действий по устранению известных эксплуатируемых уязвимостей, которые указывают на то, что организационные процессы были соблюдены и завершены в течение 48 часов с момента уведомления.

Передовые методы оценки результатов Уровня 4 включают:

* + - * + Прежде чем приступить к программе обучения, определите базовые показатели, которые можно использовать в качестве отправной точки для оценки изменений. Например, до начала программы обучения время устранения уязвимостей составляло 72 часа; После программы обучения время устранения уязвимостей составило 48 часов.
        + Используйте как количественные, так и качественные измерения, чтобы получить целостное представление о влиянии учебной программы.
        + Признайте и донесите до высшего руководства, что требуется время, чтобы увидеть полное влияние программы обучения на результаты организации.
        + Внедрите измерения и метрики для того, как атрибутировать изменения в организации с помощью программы обучения. Программа обучения в сочетании с другими организационными изменениями (например, изменением ресурсов, дополнительной поддержкой или новыми процедурами) окажет наибольшее влияние на организационные изменения.

# 5.2.4. Рассмотрение Отчета об оценке CPLP с высшим руководством

В качестве заключительного шага менеджеры CPLP встречаются со своим Комитетом высшего руководства, чтобы проанализировать эффективность программы, рассмотреть новые организационные риски или проблемы, которые следует включить в содержание учебной программы, и определить любые области, требующие значительного улучшения. В ходе проверки будут использоваться установленные измерения и требования (см.. [4.4)](#_bookmark85) для обеспечения того, чтобы подход CPLP к жизненному циклу (см. [рис. 1)](#_bookmark9) был непрерывным и непрерывным.

Во время встречи с Комитетом высшего руководства обсудите конкретные результаты и соображения, которые могут повлиять на потребности в ресурсах. Некоторым организациям может потребоваться документация, такая как проектное предложение, в котором излагается проблема (т.е. почему это необходимо), решение (т.е. что решит проблему), объем работы (т.е. резюме учебной работы), преимущества (т.е. как усилия по обучению принесут пользу сотрудникам и организации) и первоначальная оценка необходимых ресурсов (т.е. человек и финансовые затраты) на выполнение работ.

# Усилия по совершенствованию CPLP

CPLP предоставляет надежную программу обучения, предназначенную для развития знаний и навыков персонала для снижения и/или управления рисками конфиденциальности и кибербезопасности. Менеджеры CPLP и их команды должны анализировать точность, качество и уместность материалов в контексте желаемых результатов и следить за реализацией элементов, чтобы определить, соответствуют ли материалы запланированным целям.

NIST CSF [[8],](#_bookmark109) Privacy Framework и SP 800-53r5 [[11]](#_bookmark112) предлагают рекомендации, которые CPLP может адаптировать для обеспечения непрерывного мониторинга и улучшений. В категории «Улучшение» в рамках функции IDENTIFY признается важность «совершенствования процессов, процедур и действий по управлению рисками кибербезопасности в организации», а в категории «Непрерывный мониторинг» в PROTECT рассматривается мониторинг «аномалий, индикаторов компрометации и других потенциально неблагоприятных событий» (в данном случае, например, неэффективных материалов или процессов в CPLP). В категории «Мониторинг и анализ» функции GOVERN-P в рамках концепции конфиденциальности обсуждается необходимость постоянного анализа и информирования о методах управления рисками на основе этих выводов. SP 800-53r5 [[11],](#_bookmark112) раздел 1.3, включает организационную ответственность за «непрерывный мониторинг информационных систем и организаций для определения текущей эффективности средств контроля, изменений в информационных системах и средах работы, а также состояния безопасности и организации конфиденциальности

широкий». В этом контексте непрерывный мониторинг и совершенствование относятся к итеративному характеру пересмотра, обновления и поддержания программы в соответствии с требованиями и передовым опытом. Этот процесс может происходить на любом этапе CPLP и учитывает постоянно меняющиеся потребности организации в управлении ресурсами и рисками. На основе отчета об оценке CPLP и любых новых требований (например, законодательных, организационных, системных изменений, связанных с рисками и т.д.) менеджеры CPLP смогут определить возможности для улучшения.

# Сводка

В конечном счете, цель CPLP заключается в том, чтобы дать организации возможность противостоять рискам, связанным с кибербезопасностью и конфиденциальностью, для информации и активов организации. Персонал организации является важнейшей частью создания позитивных культурных норм, которые будут поддерживать цели CPLP и способствовать большему успеху в изменении поведения. Избегайте попыток наказать тех, кто не адаптируется к культуре так же хорошо, как и другие. Вместо этого пролейте свет на отдельных людей, команды и отделы, которые повышают производительность, внедряют передовые методы и помогают создать позитивную культуру CPLP. Найдите способы отметить сотрудников, которые формируют культуру CPLP в организации, и делиться информацией о работе CPLP, когда это уместно. Если обратная связь указывает на то, что необходимо внести изменения в программу обучения из-за того, что что-то не работает, убедитесь, что программа достаточно гибка для реализации этой корректировки. Не стоит ждать окончания года или другого произвольного временного промежутка.

Цели постоянного совершенствования не обязательно должны строиться на пепле прошлых неудач, их следует рассматривать как возможность для роста и укрепления критически важной программы. Позитивная культура кибербезопасности и конфиденциальности отмечает успехи, признавая при этом постоянно присутствующие риски для организации.

# Ссылки

1. Уильям М. (Мак) Торнберри Закон об ассигнованиях на национальную оборону на 2021 финансовый год, Публичный закон 116-283. Доступно в <https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf>
2. Федеральный закон о модернизации информационной безопасности 2014 года, Pub. L. 113-283, 128 Stat. 3073. Доступно в <https://www.govinfo.gov/app/details/PLAW-113publ283>
3. Административно-бюджетное управление (2016) Управление информацией как стратегическим ресурсом. (Белый дом, Вашингтон, округ Колумбия), Циркуляр OMB A-130, 28 июля 2016 года. Доступно по [https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a](https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf) [130/a130revised.pdf](https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf)
4. Де Зафра Д.Э., Питчер С.И., Тресслер Д.Д., Ипполито Дж.Б. (1998) Требования к обучению безопасности информационных технологий: модель, основанная на ролях и производительности. (Национальный институт стандартов и технологий, Гейтерсбург, штат Мэриленд), специальная публикация NIST (SP) 800-16. <https://doi.org/10.6028/NIST.SP.800-16>
5. Петерсен Р., Сантос Д., Ветцель К., Смит М., Витте Г. (2020) Workforce Framework for Cybersecurity (NICE Framework). (Национальный институт стандартов и технологий, Гейтерсбург, штат Мэриленд), специальная публикация NIST (SP) 800-181, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-181r1>
6. Хейни Дж., Джейкобс Дж., Фурман С., Барриентос Ф. (2022) Подходы и проблемы федеральных программ повышения осведомленности о кибербезопасности. (Национальный институт стандартов и технологий, Гейтерсбург, штат Мэриленд), Межведомственный или внутренний отчет NIST (IR) 8420A. <https://doi.org/10.6028/NIST.IR.8420A>
7. Хейни Дж., Джейкобс Дж., Фурман С., Барриентос Ф. (2022) Федеральная рабочая сила по повышению осведомленности о кибербезопасности: профессиональные знания, навыки и деятельность по развитию. (Национальный институт стандартов и технологий, Гейтерсберг, штат Мэриленд), внутренний отчет NIST (IR) NIST Interagency или внутренний отчет 8420B. Доступно в <https://doi.org/10.6028/NIST.IR.8420B>
8. Национальный институт стандартов и технологий (2024) Структура кибербезопасности, версия 2.0. (Национальный институт стандартов и технологий, Гейтерсберг, штат Мэриленд). <https://doi.org/10.6028/NIST.CSWP.29>
9. Национальный институт стандартов и технологий (2020) NIST Privacy Framework: инструмент для улучшения конфиденциальности с помощью управления рисками предприятия, версия 1.0. (Национальный институт стандартов и технологий, Гейтерсбург, штат Мэриленд), Белая книга по кибербезопасности NIST (CSWP) NIST CSWP 10. <https://doi.org/10.6028/NIST.CSWP.10>
10. Объединенная целевая группа (2018) Структура управления рисками для информационных систем и организаций: подход к жизненному циклу системы для безопасности и конфиденциальности. (Национальный институт стандартов и технологий, Гейтерсбург, штат Мэриленд), специальная публикация NIST (SP) 800-37,

Откр. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>

1. Объединенная целевая группа (2020) «Контроль безопасности и конфиденциальности для информационных систем и организаций». (Национальный институт стандартов и технологий, Гейтерсберг, штат Мэриленд), специальная публикация NIST (SP) 800-53, Rev. 5. Включает обновления по состоянию на 10 декабря 2020 г. <https://doi.org/10.6028/NIST.SP.800-53r5>
2. Шрёдер К., Тринх Х., Пиллиттери В. (2024) Руководство по измерениям информационной безопасности: Том 1 — Идентификация и выбор мер. (Национальный институт стандартов и технологий, Гейтерсбург, штат Мэриленд), специальная публикация NIST (SP) NIST SP 800-55v1 ipd. https://doi.org/10.6028/NIST.SP.800-55v1.ipd
3. Гранс Т., Нолан Т., Берк К., Дадли Р., Уайт Г., Гуд Т. (2006) Руководство по программам тестирования, обучения и упражнений для планов и возможностей ИТ, 1.0. (Национальный институт стандартов и технологий, Гейтерсберг, штат Мэриленд), специальная публикация NIST (SP) 800-84. Доступно в <https://doi.org/10.6028/NIST.SP.800-84>
4. Федеральный закон о модернизации информационной безопасности Генерального инспектора 2014 финансового года (FISMA) версии 1.1 (2021).Доступно в [https://www.cisa.gov/sites/default/files/publications/FY%202021%20IG%20FISMA%20](https://www.cisa.gov/sites/default/files/publications/FY%202021%20IG%20FISMA%20Metrics%20Final%20v1.1%202020-05-12.pdf) [Metrics%20Final%20v1.1%202020-05-12.pdf](https://www.cisa.gov/sites/default/files/publications/FY%202021%20IG%20FISMA%20Metrics%20Final%20v1.1%202020-05-12.pdf)
5. Киркпатрик Д.Л. (1994) Оценка программ обучения — четыре уровня (Berret-Koehler Publishers, Inc, Сан-Франциско, Калифорния).
6. Глоссарий Национального института стандартов и технологий (2024). Доступно в <https://csrc.nist.gov/glossary>
7. Закон о реформе информационных технологий 1996 года, 40 USC 11101; Раздел 5002: Определения. Доступно по адресу [https://www.govinfo.gov/content/pkg/USCODE-2021-title40/pdf/USCODE-](https://www.govinfo.gov/content/pkg/USCODE-2021-title40/pdf/USCODE-2021-title40-subtitleIII-chap111-sec11101.pdf) [2021-title40-subtitleIII-chap111-sec11101.pdf](https://www.govinfo.gov/content/pkg/USCODE-2021-title40/pdf/USCODE-2021-title40-subtitleIII-chap111-sec11101.pdf)
8. Компетенции Управления персонала США (OPM) (2024). Доступно в <https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/>

# Приложение А. Примеры уровней зрелости программы обучения по кибербезопасности и конфиденциальности

Следующий пример адаптирован из Показателей Генерального инспектора FISMA для обучения безопасности за 21 финансовый год [[14]](#_bookmark115) и предоставляет один из методов оценки зрелости программы обучения. Как и другие модели зрелости бизнеса или качества, этот пример может помочь измерить прогресс и установить стратегические цели для оптимизации программы обучения. Полностью «зрелая» программа является интегрированным операционным элементом системы и процессов и постоянно контролируется и совершенствуется.

**Таблица 3. Примеры уровней зрелости CPLP**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Вопрос** | **Специальный** | **Определенные** | **Последовательно**  **Реализованы** | **Управляемость и измеримость** | **Оптимизированные** |
| Степень, в которой роли и обязанности программы обучения были определены, доведены до сведения общественности, реализованы и обеспечены соответствующими ресурсами | Роли и обязанности не были определены, доведены до сведения или внедрены в масштабах всей организации, а также не обеспечены надлежащими ресурсами. | Роли и обязанности были определены, доведены до сведения и внедрены во всей организации, а также установлены потребности в ресурсах. | Отдельные сотрудники выполняют роли и обязанности, которые были определены во всей организации. | Ресурсы распределяются с учетом рисков, чтобы заинтересованные стороны могли последовательно реализовывать их, а заинтересованные стороны несут ответственность за эффективное выполнение своих ролей и обязанностей. | |
| Степень, в которой организация использует оценку навыков, знаний и способностей своих сотрудников для предоставления специализированного и специализированного учебного контента | Организация не определила свои процессы оценки знаний, навыков и способностей своих сотрудников. | Организация определила свои процессы оценки знаний, навыков и способностей своих сотрудников для определения своих потребностей в обучении. Компания периодически обновляет свою оценку с учетом меняющейся среды рисков. | Организация оценила знания, навыки и способности своих сотрудников; адаптировал свое учебное содержание; и выявил пробелы в навыках. Компания периодически обновляет свою оценку с учетом меняющейся среды рисков. Кроме того, оценка служит ключевым вкладом в обновление стратегии и планов обучения организации. | Организация устранила выявленные пробелы в знаниях, навыках и способностях путем обучения или привлечения талантов. | Коллективный персонал организации обладает таким уровнем подготовки, чтобы организация могла продемонстрировать, что инциденты безопасности, возникающие в результате действий или бездействия персонала, со временем сокращаются. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Вопрос** | **Специальный** | **Определенные** | **Последовательное внедрение** | **Управляемость и измеримость** | **Оптимизированные** |
| Степень, в которой организация использует стратегию и план обучения, которые основаны на оценке навыков и адаптированы к миссии организации и среде рисков. | Организация не определила свою стратегию обучения безопасности или план разработки, внедрения и поддержания программы обучения, адаптированной к ее миссии и среде риска. | Организация определила свою стратегию обучения и план разработки, внедрения и поддержания программы обучения, адаптированной к ее миссии и среде риска. | Организация последовательно реализует свою общеорганизационную стратегию и план обучения. | Организация отслеживает и анализирует качественные и количественные показатели эффективности своих стратегий и планов обучения. Организация гарантирует, что метрики, подтверждающие данные, получаются точно, последовательно и в воспроизводимом формате. | Мероприятия по программе обучения организации интегрированы в другие области, связанные с безопасностью. Например, общие риски, слабые места в контроле и другие результаты деятельности агентства по управлению рисками и постоянному мониторингу информируют о любых обновлениях, которые необходимо внести в программу обучения. |
| Степень, в которой организация гарантирует, что программа обучения предоставляется всем сотрудникам и адаптирована на основе ее миссии, среды рисков и типов информационных систем | Организация не определила свои политики, процедуры обучения или связанные с ними материалы на основе своей миссии, среды риска или типов информационных систем, к которым ее учащиеся имеют доступ.  Организация не определила свои процессы для обеспечения того, чтобы весь персонал проходил обучение при первоначальном доступе к системе и периодически в дальнейшем.  Организация не определила свои процессы оценки или получения обратной связи по своей программе обучения, чтобы постоянно совершенствоваться. | Организация определила и адаптировала свои политики обучения, процедуры, соответствующие материалы и методы обучения на основе выявленных требований и типов информационных систем, к которым ее учащиеся имеют доступ.  Организация определила свои процессы для обеспечения того, чтобы весь персонал, включая подрядчиков, проходил обучение при первоначальном доступе к системе и периодически в дальнейшем.  Организация определила свои процессы оценки и получения отзывов о своей программе обучения и использует эту информацию для постоянного совершенствования. | Организация обеспечивает последовательное внедрение своих политик и процедур обучения.  Организация гарантирует, что все соответствующие учащиеся завершают обучение организации при первоначальном доступе к системе и периодически в дальнейшем, а также ведет записи о прохождении обучения.  Организация получает обратную связь о своей программе обучения и использует эту информацию для внесения улучшений. | Организация измеряет эффективность своей программы обучения, например, путем проведения практических занятий и последующей дополнительной осведомленности, обучения или дисциплинарных мер, в зависимости от обстоятельств.  Организация отслеживает и анализирует качественные и количественные показатели эффективности своей политики, процедур и практики обучения.  Организация гарантирует, что метрики, подтверждающие данные, получаются точно, последовательно и в воспроизводимом формате. | Организация институционализировала процесс постоянного совершенствования, который включает в себя передовые методы обучения и технологии.  В режиме, близком к реальному времени, организация активно адаптирует свои политики, процедуры и процессы обучения к меняющемуся ландшафту кибербезопасности и конфиденциальности и предоставляет учебные материалы о развивающихся и сложных угрозах и проблемных действиях с данными, если это необходимо. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Вопрос** | **Специальный** | **Определенные** | **Последовательное внедрение** | **Управляемость и измеримость** | **Оптимизированные** |
| Степень, в которой организация обеспечивает предоставление специализированного обучения лицам, несущим значительную ответственность за безопасность или неприкосновенность частной жизни | Организация не определила свои политики, процедуры обучения по безопасности и конфиденциальности или связанные с ними материалы на основе своей миссии, среды риска или типов ролей, несущих значительные обязанности по обеспечению безопасности или конфиденциальности.  Организация не определила свои процессы для обеспечения того, чтобы сотрудники, выполняющие важные функции и обязанности в области безопасности или конфиденциальности, получали специализированное учебное содержание и не предлагали дополнительных возможностей для обучения. | Организация определила свои политики обучения безопасности и конфиденциальности, процедуры и связанные с ними материалы на основе своих требований, миссии, среды рисков и типов ролей со значительными обязанностями в области безопасности и конфиденциальности.  Организация определила свои процессы для обеспечения того, чтобы сотрудники, которым назначены роли и обязанности в области безопасности и конфиденциальности, получали специализированные учебные материалы по безопасности и периодически предоставляли дополнительные возможности для обучения. | Организация следит за тем, чтобы ее политики и процедуры обучения в области безопасности и конфиденциальности последовательно выполнялись.  Организация гарантирует, что лица, несущие значительные обязанности в области безопасности и неприкосновенности частной жизни, завершают специализированное обучение, определенное организацией, и им предоставляются периодические усовершенствования или дополнительные возможности для обучения.  Организация ведет учет завершений специализированного обучения, пройденного лицами, выполняющими значительные обязанности в области безопасности и конфиденциальности.  Организация получает отзывы о своей программе обучения безопасности и конфиденциальности и использует эту информацию для внесения улучшений. | Организация следит за тем, чтобы ее политики и процедуры обучения в области безопасности и конфиденциальности последовательно выполнялись.  Организация гарантирует, что лица, несущие значительные обязанности в области безопасности и конфиденциальности, пройдут специализированное обучение организации по безопасности и конфиденциальности, а также предоставляет периодические усовершенствования и дополнительные возможности для соответствующего обучения.  Организация ведет учет завершений специализированного обучения, пройденного лицами, выполняющими значительные обязанности в области безопасности и конфиденциальности.  Организация получает отзывы о своей программе обучения безопасности и конфиденциальности и использует эту информацию для внесения улучшений. | Организация институционализировала процесс постоянного совершенствования, который включает в себя передовые методы и технологии обучения безопасности и конфиденциальности.  В режиме, близком к реальному времени, организация активно адаптирует свои политики, процедуры и процессы обучения безопасности и конфиденциальности к меняющемуся ландшафту кибербезопасности и конфиденциальности и предоставляет учебные материалы по развивающимся и сложным угрозам и проблемным действиям с данными, если это необходимо. |

# Приложение Б. Глоссарий

В данной специальной публикации используются следующие термины, а некоторые определения взяты из их первоисточников. Дополнительные термины, которые не определены ниже, можно найти в глоссарии NIST [[16]](#_bookmark117).

**осознание**

Способность пользователя распознавать и избегать поведения, которое может поставить под угрозу кибербезопасность, а также действовать мудро и осторожно для повышения кибербезопасности.

**Содержание осведомленности**

Содержимое, разработанное и внедренное для того, чтобы помочь сотрудникам понять, как их действия могут повлиять на уязвимости и угрозы. Организации предоставляют различные типы информационных материалов (например, плакаты, информационные бюллетени, веб-сайты), чтобы сотрудники могли осознать свою роль в защите киберактивов.

**Тренинг по повышению осведомленности**

Базовая программа обучения кибербезопасности или конфиденциальности для всего персонала. Он предназначен для того, чтобы помочь учащимся понять роли, которые они играют в защите информации, кибербезопасности и активов, связанных с конфиденциальностью. Он часто состоит из онлайн-курсов под руководством инструктора, упражнений или других методов, которые информируют учащихся о допустимом использовании систем организации и рисках для них.

*Примечание:* Это называется обучением «грамотности» в семействе SP 800-53r5 [[11]](#_bookmark112) Awareness and Training (AT).

Также см. *обучение*.

**сертификация**

Звание, полученное для обеспечения квалификации для выполнения работы или задачи. Часто выдается профессиональной организацией, отраслевым поставщиком или работодателем для обозначения достижений после курса обучения.

**Директор по искусственному интеллекту**

Высшее руководитель, отвечающее за координацию использования искусственного интеллекта (ИИ) в своем ведомстве, продвижение инноваций в области ИИ в своем ведомстве и управление рисками, связанными с использованием ИИ в своем ведомстве.

**Директор по данным**

Руководитель высшего звена, отвечающий за использование и управление данными в агентстве или организации.

**Финансовый директор**

Старший член, ответственный за управление финансовыми действиями агентства или организации.

**Директор по обучению**

Руководитель высшего звена, который контролирует все программы обучения и развития сотрудников в агентстве или организации.

**Директор по конфиденциальности**

Старшее должностное лицо, назначенное руководителем каждого агентства для выполнения обязанностей по обеспечению неприкосновенности частной жизни в масштабах всего агентства, включая реализацию мер по защите неприкосновенности частной жизни, соблюдение федеральных законов, нормативных актов и политик, связанных с неприкосновенностью частной жизни, управление рисками в отношении конфиденциальности в агентстве, а также центральную роль в разработке и оценке агентством законодательных, нормативных и других политических предложений.

**компетенция**

Способность человека выполнять задачу или задачи в контексте рабочей роли.

Из OPM: « *Компетенция* — это измеримый набор знаний, навыков, способностей, поведения и других характеристик, которые необходимы человеку для успешного выполнения рабочих или профессиональных функций.

Компетенции определяют, «как» выполнять рабочие задачи, или что нужно человеку для успешного выполнения работы. [[18]](#_bookmark118)

**конфиденциальность**

Сохранение санкционированных ограничений на доступ к информации и ее раскрытие, включая средства защиты частной жизни и служебной информации.

**Менеджер(ы) CPLP (Программа обучения кибербезопасности и/или конфиденциальности)**

Лицо или лица в организации, ответственные за разработку, закупку, интеграцию, изменение, эксплуатацию, обслуживание или окончательное размещение элементов учебных программ по кибербезопасности и/или конфиденциальности (CPLP). В некоторых организациях существует несколько итераций учебных программ, в которых кибербезопасность и конфиденциальность управляются отдельно.

**Киберполигон**

Этот метод обеспечивает безопасную среду (т.е. «песочницу») для проведения практических реалистичных тренингов, сценариев, задач и упражнений в легкодоступной веб-среде.

**Кибербезопасность**

Предотвращение, повреждение, защита и восстановление компьютеров, электронных коммуникационных систем, услуг электронной связи, проводной связи и электронных коммуникаций, включая содержащуюся в них информацию, для обеспечения их доступности, целостности, аутентификации, конфиденциальности и неопровержимости.

**Конфиденциальность данных**

Состояние, которое гарантирует человеческую автономию и достоинство с помощью различных средств, включая конфиденциальность, предсказуемость, управляемость и диссоциацию.

**Специалист по управлению данными**

Должностное лицо, ответственное за контроль и выполнение задач по управлению данными исследовательских проектов. Основные обязанности и ответственность включают сбор данных или разработку, внедрение и обеспечение соблюдения надлежащих политик и процедур сбора данных. Обучает отчетные агентства инструментам и оборудованию для сбора данных.

**Диссоциативность**

Обеспечение обработки данных или событий без связи с отдельными лицами или устройствами, выходящими за рамки эксплуатационных требований системы.

**Анализ пробелов**

Процесс сравнения текущей учебной программы или эффективности деятельности с желаемыми, ожидаемыми результатами.

**информационная технология**

Любое оборудование или взаимосвязанная система или подсистема оборудования, используемая для автоматического сбора, хранения, анализа, оценки, манипулирования, управления, перемещения, контроля, отображения, коммутации, обмена, передачи или приема данных или информации исполнительным органом, если оборудование используется исполнительным агентством непосредственно или используется подрядчиком по контракту с исполнительным агентством, который требует использования (i) этого оборудования или (ii) этого оборудования для значительный объем в выполнении услуги или предоставлении товара. Включает компьютеры, вспомогательное оборудование (включая периферийные устройства обработки изображений, устройства ввода, вывода и хранения, необходимые для обеспечения безопасности и наблюдения), периферийное оборудование, предназначенное для управления центральным процессором компьютера, программное обеспечение, микропрограммное обеспечение и аналогичные процедуры, услуги (включая услуги поддержки) и связанные с ними ресурсы. Не включает оборудование, приобретенное федеральным подрядчиком в связи с федеральным контрактом.

**целостность**

Защита от неправомерного изменения или уничтожения информации, а также обеспечение неопровержимости и подлинности информации.

**Цели обучения**

Определяет результаты, которые должен быть достигнут в рамках подкомпонента или модуля программы обучения для каждого из участников, а также связанные с ними роли в снижении, управлении и смягчении рисков.

**Программа обучения**

Состоит из многочисленных элементов под руководством менеджеров программ обучения, которые разрабатывают стратегический план для реализации программы правильного размера по снижению рисков кибербезопасности и конфиденциальности организации посредством обучения и подготовки персонала. Работает в течение всего года и включает в себя планы по постоянным улучшениям, основанные на строгих оценках и показателях, поддерживающих соответствие требованиям и другую обязательную отчетность.

**План учебной программы**

Официальный документ, в котором представлен обзор программы обучения по кибербезопасности и конфиденциальности агентства, включая описание ее структуры, выделенных для нее ресурсов, ролей старших должностных лиц и сотрудников агентства, а также стратегических целей и задач программы обучения для соблюдения применимых требований к конфиденциальности и управления рисками конфиденциальности.

**грамотность**

Знакомство человека с базовым набором знаний.

**управляемость**

Предоставление возможности детального управления данными, включая изменение, удаление и выборочное раскрытие.

**Оценка потребностей**

Процесс выявления пробелов в обучении и потребностей учебной деятельности.

**предсказуемость**

Предоставление физическим лицам, владельцам и операторам надежных предположений о данных и их обработке системой, продуктом или услугой.

**Мероприятие по обеспечению конфиденциальности**

Возникновение или потенциальное возникновение проблемных действий с данными.

**Привилегированный сетевой аккаунт**

Сетевая учетная запись с повышенными привилегиями, которая обычно назначается системным администраторам, сетевым администраторам, администраторам баз данных и другим лицам, отвечающим за функции управления, мониторинга или администрирования системы и приложений.

**Владелец учетной записи с привилегированным доступом**

Пользователь, который уполномочен (и, следовательно, ему доверяют) выполнять функции, связанные с безопасностью, которые обычные пользователи не имеют права выполнять (например, специальный доступ к программным приложениям или веб-публикациям), требует дополнительного обучения и должен подписать политику допустимого использования. Пользователь с учетной записью с привилегированным доступом.

**Проблемное действие с данными**

Действие с данными, которое может привести к неблагоприятным последствиям для отдельных пользователей.

**Метрики программы**

Инструменты, предназначенные для облегчения принятия решений и повышения эффективности и подотчетности за счет сбора, анализа и отчетности соответствующих данных, связанных с результатами деятельности.

**Обучение на основе ролей**

Многоступенчатый процесс в программе обучения, который начинается с определения основных рабочих ролей в области кибербезопасности или конфиденциальности в организации и определения персонала, соответствующего этим назначенным рабочим ролям. Затем учебные материалы назначаются, приобретаются или разрабатываются на основе задач, необходимых для выполнения рабочей роли. (См. Фреймворк NICE [[3]](#_bookmark104) для «рабочей роли».)

*ПРИМЕЧАНИЕ:* Кроме того, SP 800-53r5 [[11]](#_bookmark112) control AT-3 дает следующее определение ролевого обучения: «Комплексное ролевое обучение охватывает управленческие, оперативные и технические роли и обязанности, охватывающие физический, кадровый и технический контроль. Обучение на основе ролей также включает в себя политики, процедуры, инструменты, методы и артефакты для определенных ролей кибербезопасности и конфиденциальности.

Организации проводят обучение, необходимое для выполнения ими своих обязанностей, связанных с операциями и управлением рисками в цепочке поставок в контексте программ кибербезопасности и конфиденциальности организации. Обучение на основе ролей также распространяется на подрядчиков, которые предоставляют услуги федеральным агентствам».

**Старший сотрудник агентства по вопросам конфиденциальности**

Старшее должностное лицо, назначенное руководителем каждого агентства, которое несет ответственность за неприкосновенность частной жизни в масштабах всего агентства, включая реализацию мер по защите неприкосновенности частной жизни; обеспечение соблюдения федеральных законов, нормативных актов и политик, связанных с неприкосновенностью частной жизни; управление рисками конфиденциальности в агентстве; и выполнение центральной роли в разработке и оценке агентством законодательных, нормативных и других политических предложений.

**Значительные обязанности в области кибербезопасности или неприкосновенности частной жизни**

Предпочтительная терминология в настоящем документе для определения тех, чьи роли в организации требуют постоянного ролевого обучения. Эти лица имеют обязанности, связанные с работой, помимо обязанностей всех пользователей, и должны будут участвовать как в общей, так и в специализированной учебной программе.

*ПРИМЕЧАНИЕ:* Из FISMA FY2014 CIO Metrics [[14]:](#_bookmark115) «К числу тех, кто несет значительные обязанности в области кибербезопасности, относятся все пользователи, у которых есть одна или несколько привилегированных учетных записей пользователей сети, и все остальные пользователи, которые имеют управленческие или операционные обязанности, позволяющие им повышать или уменьшать кибербезопасность».

**синхронное обучение**

Обучение, в котором инструкторы и учащиеся должны участвовать вместе в виртуальной или физической учебной среде.

**Материалы столешниц**

Материалы, разработанные для дискуссионного упражнения, в котором сотрудники, выполняющие роли и обязанности в определенном ИТ-плане, встречаются в классе или в группах для обсуждения своих ролей во время чрезвычайной ситуации и реагирования на конкретную чрезвычайную ситуацию. Фасилитатор начинает обсуждение, представляя сценарий и задавая вопросы, основанные на этом сценарии.

*ПРИМЕЧАНИЕ:* В SP 800-84 [[13]](#_bookmark114) командно-штабные упражнения обычно включают в себя следующую документацию:

* Брифинг для участников, который включает в себя повестку дня и информацию о логистике.
* Руководство для фасилитаторов, которое включает в себя:
  + Цель проведения учения
  + Сфера охвата и цели учения
  + Сценарий учения, представляющий собой последовательный повествовательный рассказ о гипотетическом инциденте, который служит катализатором для учения и предназначен для представления ситуаций, которые вдохновят на реакцию и позволят продемонстрировать цели учения
  + Список вопросов по сценарию, которые относятся к целям учения
  + Копия выполняемого ИТ-плана

Типы вопросов, задокументированные в руководстве для фасилитатора, должны быть адаптированы к участникам. Например, если участниками являются сотрудники высшего звена, вопросы должны носить более общий характер и быть сосредоточенными на принятии решений и надзоре, которые согласуются с их ролями и обязанностями в рамках плана. Если участниками является оперативный персонал, вопросы, как правило, должны быть сосредоточены на конкретных процедурах и процессах выполнения ролей и обязанностей.

* Руководство для участников, содержащее ту же информацию, что и руководство для фасилитатора, с измененным, более коротким списком вопросов, чтобы сориентировать участников на типы проблем, которые могут обсуждаться во время упражнения.
* Отчет о действиях

**тренировка**

Инструктаж или учебная деятельность, направленная на повышение способности работника выполнять конкретные должностные функции и задачи путем сосредоточения внимания на навыках, концепциях, знаниях и отношениях, связанных с выполнением работы. Он призван изменить то, что сотрудники знают и как они работают.

*ПРИМЕЧАНИЕ:* Ссылки на обучение в законодательстве США: См. Кодекс США § 4101 – Определения [[15]:](#_bookmark116) (4) «обучение» означает процесс обеспечения и предоставления работнику возможности, а также размещения или зачисления работника в запланированную, подготовленную и скоординированную программу, курс, учебный план, предмет, систему или рутину обучения или образования в научной, профессиональной, технической, механической, профессиональной, профессиональной, механической, профессиональной деятельности, канцелярских, финансовых, административных или других областях, которые улучшат индивидуальную и организационную эффективность и помогут в достижении миссии и целей деятельности агентства.

**Виртуальный светодиод**

Когда обучение происходит в виртуальной или смоделированной среде и представляется или проводится инструктором в режиме реального времени.

**Предупреждающий баннер**

Начальный экран, который информирует пользователей о последствиях доступа к компьютерному ресурсу (например, согласие на мониторинг). Охранный баннер. Уведомление об использовании системы.

**Обучение через Интернет**

Интернет-сессия, которая позволяет учащимся учиться самостоятельно и в удобном для них темпе с использованием видео, аудио и/или интерактивных методов (например, перетаскивание или заполнение пробелов). Встроенные функции тестирования и отчетности позволяют измерять производительность.

**Рабочая роль**

Группировка работ, за которую кто-то несет ответственность. Не является синонимом названия должности или профессии, хотя они могут совпадать, в зависимости от организации. Например, рабочая роль «разработчика программного обеспечения» может применяться к тем, кто имеет разные названия должностей, таким как инженеры-программисты, программисты и разработчики приложений. И наоборот, несколько ролей могут быть объединены для создания определенной работы. Этот аддитивный подход поддерживает улучшенную модульность и иллюстрирует тот факт, что все учащиеся в рабочей силе выполняют множество задач в различных ролях, независимо от их должностей.

# Приложение В. Журнал изменений

В сентябре 2024 года в отчет были внесены следующие изменения:

* Была включена дополнительная информация для удовлетворения требований, изложенных в циркуляре АБУ A-130.
* В этом руководстве используются другие соответствующие публикации NIST, выпущенные за последние 20 лет, такие как NIST Cybersecurity Framework, NIST Risk Management Framework, NIST Privacy Framework.
* Терминология была адаптирована к стандартизированному языку, найденному в NICE Workforce Framework for Cybersecurity. Участники программы называются «учащимися», а общая программа теперь называется «учебной программой».
* В этой публикации рассматриваются вопросы, которые были выявлены в ходе исследований NIST с федеральными специалистами по обучению кибербезопасности и конфиденциальности (например, руководство по разработке эффективных метрик и измерений).