ПАКЕТ ИНСТРУМЕНТОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ:

защита исполнителей и улучшение результатов программы

Руководство и инструменты для укрепления безопасности в рамках программ для ключевых групп населения, поддерживаемых Глобальным фондом

БЛАГОДАРНОСТИ

Настоящий пакет инструментов был разработан Институтом гражданского общества в области здравоохранения стран Западной и Центральной Африки (CSIH-WCA) и организацией FHI 360. Он основывается на инструментах для обеспечения безопасности и руководствах, разработанных организацией FHI 360 и ее партнерами в рамках проектов LINKAGES и EpiC, финансируемых USAID и PEPFAR. Эти инструменты были пересмотрены с учетом конкретных потребностей и реалий программ, осуществляемых при поддержке Глобального фонда в Западной и Центральной Африке. Работа по адаптации данных инструментов была произведена в 2022 году при участии программ и организаций, взаимодействующих с ключевыми группами населения в регионе Западной и Центральной Африки. Поддержку в адаптации указанных инструментов оказал департамент по работе с сообществами, правам человека и гендерным вопросам Глобального фонда по борьбе со СПИДом, туберкулезом и малярией. Мы благодарим следующие организации за их вклад в этот процесс:

Буркина-Фасо
AIDSETI
AVP
AWEYA
CPCNLS

Камерун
инициатива "Равноправие"
CHP
Empower-Cameroun
ESPOIR+
Ndop
Reach Out

Сенегал
AJDPASTEEF
ANCS
APCSID
ENDA Sante
ONG AWA
ONG 3D
RENAPOC
RNP+

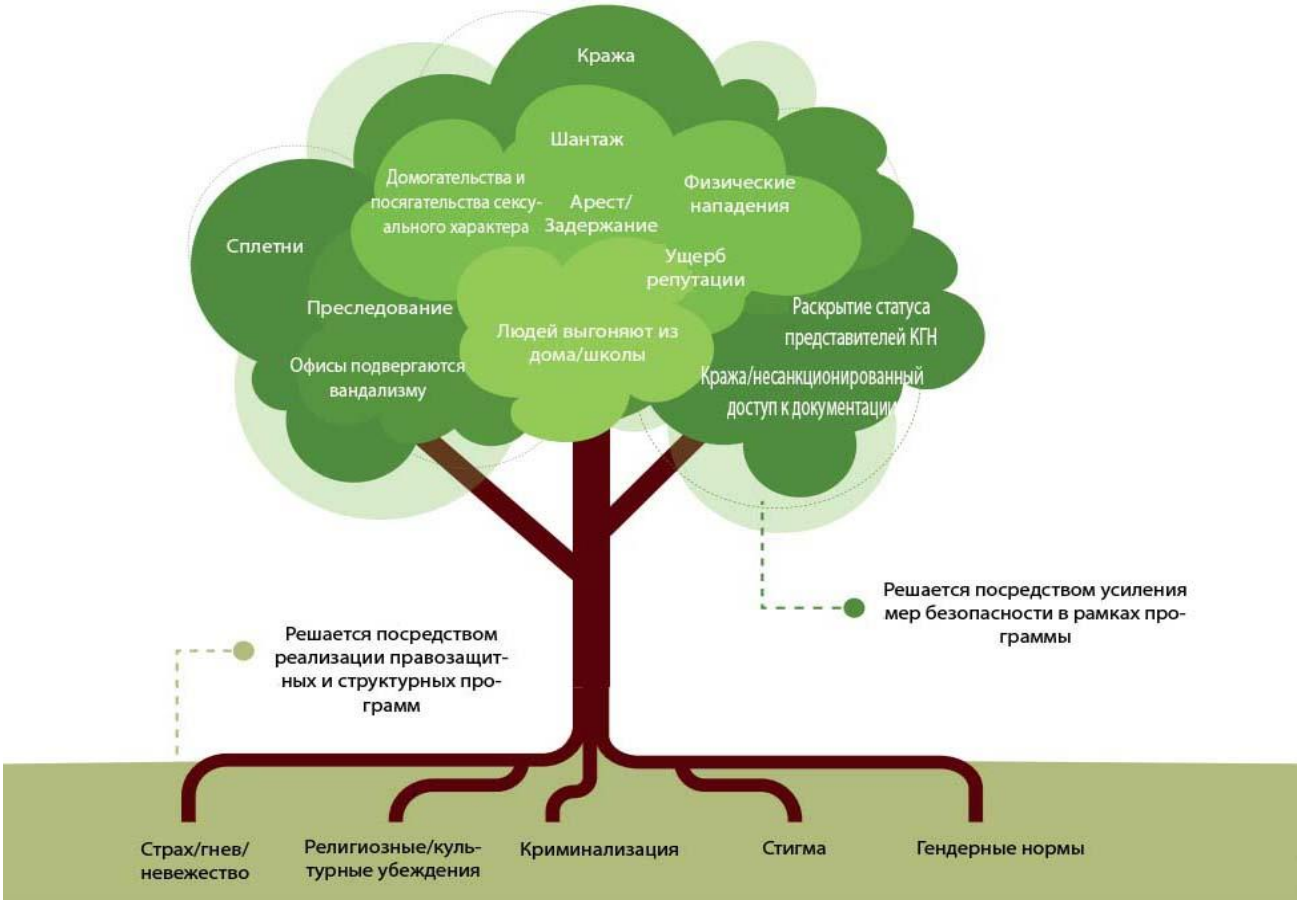
Сьерра-Леоне
"Достоинство"
IHPAU
RODA
SLYDCL
SWAASL
"Женщины в кризисе"

ОГЛАВЛЕНИЕ

Часть 1: РУКОВОДСТВО ПО ИСПОЛЬЗОВАНИЮ ИНСТРУМЕНТОВ

Сведения общего характера.

Риски и барьеры, связанные с правами человека, с которыми сталкиваются ключевые группы населения, хорошо известны, и их устранение считается важным компонентом комплексной программы по ВИЧ для ключевых групп населения. Связанной с этим, но менее понятной проблемой является безопасность тех, кто участвует в реализации программ по ВИЧ для ключевых групп населения и в предоставлении услуг этим группам. Организации-исполнители, в которых зачастую ведущую роль играют представители ключевых групп населения, часто подвергаются угрозам и нападениям с применением насилия, которые напрямую связаны с их работой. Такая незащищенность тяжело отражается на физическом и психическом здоровье сотрудников программ. Эти проблемы снижают эффективность этих программ, поскольку они связаны с арестами сотрудников, ущербом для репутации организации, ограничением свободы передвижения и несанкционированным доступом к данным, а также с другими проблемами, которые отвлекают внимание от реализации программ, ограничивают охват программ и могут вынудить бенефициаров программ избегать получения таких услуг.



Хотя программы по правам человека используют долгосрочный подход к устранению коренных причин насилия, стигмы, дискриминации и нарушений прав человека, включая работу на политическом и законодательном уровне, также жизненно важно осуществлять повседневные действия для снижения риска угроз безопасности и инцидентов, с которыми сталкиваются программы, и реагирования на них в случае их возникновения. Систематическое отслеживание и оценка рисков, а также выделение ресурсов и принятие мер для снижения этих рисков и реагирования на инциденты являются неотъемлемой частью любой программы по ВИЧ для ключевых групп населения, имеют важное значение для достижения и поддержания результатов в программах по ВИЧ и правам человека. Крайне необходимо заботиться о безопасности организаций, работающих на переднем крае, их работниках и волонтерах. Это также важно для того, чтобы сделать программы под руководством сообщества безопасным и устойчивым вариантом получения услуг.

Глобальный фонд для борьбы со СПИДом, туберкулезом и малярией сотрудничает с FHI 360 и Институтом гражданского общества в области здравоохранения стран Западной и Центральной Африки (CSIH-WCA) для адаптации инструментов, которые программы могут использовать для прогнозирования рисков в сфере безопасности, составления планов на будущее для снижения этих рисков и реагирования на инциденты и угрозы. В этом документе представлены инструменты, доступные исполнителям программ Глобального фонда. Их можно использовать для систематического включения мер безопасности в существующие программы, а также в качестве основы для выделения ресурсов на цели обеспечения безопасности в рамках процессов корректировки программ или странового диалога.

Примеры проблем в области безопасности программ

Организации ключевых групп населения, участвующие в разработке этих инструментов, описали широкий спектр различных угроз безопасности или инцидентов, связанных с тем, что злоумышленники *намеренно* угрожают или предпринимают действия против программы из-за ее связи с ВИЧ и ключевыми группами населения. Примеры угроз и инцидентов, с которыми часто сталкиваются организации и программы, работающие с ключевыми группами населения, включают:

- Кампании в СМИ против ОГО, в которых руководство и персонал ОГО характеризовались как лица, пропагандирующие гомосексуальность и проституцию, что привело к социальному остракизму работников ОГО и нанесло вред их психическому здоровью. Организация была вынуждена закрыться на несколько недель, ограничив доступ к услугам по ВИЧ до тех пор, пока не утихли волны народного гнева.
- Человек, представившийся бенефициаром, пришел в ОГО, предоставляющее услуги представителям КГН, и снял на видео процесс раздачи презервативов. Затем этот человек разместил видео в Интернете и заявил, что данная организация гражданского общества занимается незаконной и аморальной деятельностью. Эта ОГО подверглась нападению разгневанных соседей, и ей пришлось на время прекратить свою деятельность.
- Аутрич-работника посадили на несколько дней в тюрьму за то, что у него были обнаружены презервативы. После освобождения данный работник был отвергнут членами семьи и стал бездомным. Это повлияло как на трудоспособность человека, так и на моральное состояние других аутрич-работников.
- Бенефициары начали злиться на работников ОГО и словесно оскорблять их, когда ОГО не смогла удовлетворить их комплексные потребности, такие как продовольственная помощь. Сотрудники ОГО испытывали психологический стресс и страх за свою физическую безопасность. В некоторых случаях работники уходили из организации из-за стресса.
- Аутрич-работников арестовывали по ложному обвинению в принуждении к сексу при раздаче презервативов,

что ограничивало их способность эффективно доставлять соответствующие товары.

- Мобильный автобус для тестирования чуть не был перевернут, когда экстремистски настроенные студенты университета собрались в толпу в знак протеста против пропаганды использования презервативов, которую они считали аморальной. Это ограничило возможность проведения аутрич мероприятий в данном районе.
- Веб-сайт ОГО был взломан, и против него были организованы онлайн-кампании троллинга после того, как ОГО попыталась снизить стигматизацию в отношении представителей КГН посредством публичных сообщений. Деньги приходилось отвлекать от других программ или получать путем дополнительного сбора средств для повышения кибербезопасности.
- Из центров доверия поступали сообщения о словесных оскорблениях, кражах, а иногда и о физических нападениях на персонал исполнителей программы, включая врачей. Это привело к стрессу, экономическому ущербу и текучести кадров.
- Семья бенефициара узнала, что их ребенок получает услуги от ОГО, которая занимается снижением риска заражения ВИЧ среди представителей КГН. Семья обвинила ОГО в торговле людьми и попыталась возбудить уголовное дело. Репутация ОГО пострадала, и сотрудникам пришлось тратить свое время на опровержение ложного обвинения.
-

Ключевые рекомендации по обеспечению безопасности программы

Эти рекомендации были разработаны на основе консенсуса представителей программ для ключевых групп населения по всему миру в ходе работы над повышением их безопасности. Они актуальны не только для программ, работающих непосредственно с бенефициарами, но и для основных получателей, субполучателей и Глобального фонда. Они представлены здесь, чтобы улучшить ваше общее представление о безопасности.

- Сделать принципы и подходы программ по ВИЧ основой усилий по обеспечению безопасности. К ним относятся следующие принципы: «ничего о нас без нас» и «прежде всего, не навреди».
- Сделать безопасность приоритетом и явным образом обеспечить ее ресурсами.
- Обязанностью организации является создать безопасное рабочее место, в том числе такое, которое обеспечивает охрану и сохранение психического здоровья.
- Планировать заранее и убедиться, что все знают план (сохраняя при этом гибкость).
- Подробно обсудить уровень риска, который приемлем для организации и отдельных сотрудников.
- Действовать, зная как реальные риски, так и их основные причины (включая правовую базу).
- Осознавать различные факторы уязвимости и возможности каждого работника при планировании безопасности.
- Хорошо узнать все заинтересованные стороны, а не только очевидных союзников.
- Определять как угрозы (физические, цифровые, психологические), так и стратегии безопасности в комплексе.
- Взаимодействовать с другими программами, работать в коалиции и учиться друг у друга.

Обзор инструментов

Что мы подразумеваем под безопасностью программы?

Безопасность программы заключается в сокращении случаев *преднамеренного* насилия и угроз в адрес программы и всех ее участников и реагировании на такие случаи. Для программ по ВИЧ для ключевых групп населения это обычно связано с тем, что программы подвергаются угрозам или нападениям именно потому, что они работают в сфере ВИЧ с ключевыми группами населения. Причины и лица, совершающие такие действия, могут быть разными, но источником этих угроз и нападений часто является стигматизация и неприятие ключевых групп населения.

Для чего нужны инструменты?

Эти инструменты предназначены для того, чтобы помочь организациям, участвующим в реализации программ по ВИЧ для ключевых групп населения:

- систематически определять свои возможности, сильные и слабые стороны в области безопасности;
- определять приоритетные риски, которые необходимо устранить, и отслеживать угрозы для своей организации и работников;
- составлять планы, которые позволят им снизить эти риски и угрозы или снизить их уязвимость в отношении таких рисков и угроз;
- и обеспечить эффективное реагирование при возникновении инцидентов.

Многие стратегии по повышению безопасности программ предполагают изменение методов работы организации или принятие мер по снижению рисков. В некоторых случаях может также возникнуть необходимость включить в программу новые мероприятия – например, более активную информационно-разъяснительную работу с представителями местных органов власти и органами безопасности – или закупить оборудование или оплатить услуги и нанять специалистов, которые помогут повысить безопасность. Эти расходы являются приемлемыми для финансирования Глобальным фондом, поэтому важно убедиться, что они включены в запросы на финансирование Глобального фонда, а также в субгранты или субконтракты с организациями-исполнителями, работающими непосредственно с бенефициарами. Таким образом, результаты использования этих инструментов могут учитываться при планировании и составлении бюджета грантов Глобального фонда.

Кому следует использовать эти инструменты?

Проблемы безопасности, с которыми сталкиваются программы по ВИЧ для ключевых групп населения, очень специфичны для каждой организации и места, где реализуются программы. Действия, необходимые для снижения проблем безопасности, также специфичны для каждой организации и местоположения. Даже если различные программы для ключевых групп населения сталкиваются с одинаковыми угрозами и инцидентами, важно, чтобы они находили решения, которые работают для них.

По этой причине эти инструменты предназначены в первую очередь для использования организациями, работающими на переднем крае реализации программ, например, в сфере поддержки лечения ВИЧ, обучения «равный-равному» или правозащитной работы для ключевых групп населения.

В программах, поддерживаемых Глобальным фондом, эти ведущие организации часто получают средства не напрямую от Глобального фонда, а от основных получателей (ОП) или субполучателей (СП). ОП и СП играют

роль в поддержке и укреплении потенциала организаций, работающих на передовой линии, особенно если они являются организациями под руководством сообществ. Таким образом, ОП и СП могут также использовать эти инструменты обеспечения безопасности программ для облегчения планирования мер безопасности с организациями, работающими на передовой линии, которые они поддерживают. Кроме того, многие ОП и СП сами сталкиваются с рисками безопасности, и поэтому они также могут использовать эти инструменты, чтобы обеспечить максимальную безопасность своей работы.

Краткое описание инструментов и процессов планирования безопасности

Каждый из инструментов в этом пакете по-своему полезен для организаций, участвующих в программах по ВИЧ для ключевых групп населения. Использование только одного из инструментов, вероятно, будет полезным с точки зрения улучшения того, как программа относится к проблемам безопасности и как она действует для их устранения.

В то же время эти инструменты можно также рассматривать как различные этапы процесса планирования, которые приведут к эффективному внедрению мер безопасности в запросы на финансирование и гранты Глобального фонда. Этот процесс и соответствующие инструменты представлены на схеме ниже.

Полезные ресурсы

https://www.fhi360.org/resource/aman-mena-toolkit

https://www.fhi360.org/resource/implementer-and-data-security

https://www.fhi360.org/resource/when-situations-go-bad-worse-guidance-international-and-regional-actors-responding-acute

https://www.fhi360.org/sites/default/files/media/documents/resource-secure-mobile-devices-apps.pdf

https://www.fhi360.org/sites/default/files/media/documents/resource-linkages-safety-security-toolkit.pdf

ЧАСТЬ 2: ИНСТРУМЕНТЫ

Инструмент 1: Журнал инцидентов в области безопасности

Описание

Этот инструмент предоставляет собой шаблон для систематической регистрации инцидентов в области безопасности, включая угрозы, с которыми сталкивается организация или отдельные лица, работающие в программе. Пользователи могут описать инцидент: когда и почему он произошел, и кто стал его причиной, а также ряд других подробностей. В нем могут фиксироваться закономерности с точки зрения типов инцидентов или лиц, их вызывающих, или даже времени (года, недели или дня), когда инциденты происходят чаще всего. Это полезно, поскольку позволяет организации со временем понять, какие типы инцидентов происходят и как лучше их предотвращать и реагировать на них. Журнал также можно использовать для обмена информацией с другими аналогичными организациями, чтобы предупредить их о возможных угрозах, а также для обмена информацией со спонсорами, чтобы побудить их покрыть расходы на повышение безопасности. Это может помочь определить:

- Более рискованные места или виды деятельности
- Лиц, часто вызывающих инциденты
- Представляет ли данный инцидент или угроза также и косвенную угрозу для других
- Повышается ли уровень насилия
- Кто подвергается наибольшему риску

Как это использовать

Журнал можно использовать по-разному, и каждая организация должна определить, что ей подходит. Инструмент, содержащийся в этом пакете, представлен в виде таблицы в формате MS Word. Пользователи могут создавать новый экземпляр таблицы (в электронном или бумажном виде) для каждого инцидента. Если используются электронные версии, пользователи должны решить, копировать и вставлять таблицу в один и тот же документ или сохранять новый файл для каждого инцидента. Наиболее важно хранить записи обо всех инцидентах в одном месте (например, в специальной электронной папке). Другой вариант — перенести инструмент в формат базы данных или Excel, чтобы хранить информацию в одном месте. Если используются печатные копии, каждая новая форма также должна храниться в одном и том же месте. В обоих случаях информация должна храниться в безопасности, например, в виде защищенного паролем или зашифрованного файла (в электронном виде) или в запертом шкафу (бумажная копия).

Пользователи также должны решить, кто будет заполнять журналы, и кто будет их анализировать. Лица, непосредственно пострадавшие от инцидента, всегда должны участвовать в заполнении журнала, однако организация может решить, будет ли это лицо делать это самостоятельно или ему будет помогать другое лицо. Не собирайте идентифицирующую информацию в формах без разрешения лица, сообщившего об инциденте. Полезно иметь в организации координатора, отвечающего за хранение и анализ данной информации. Одним из способов использования информации является периодический анализ всех инцидентов (например, во время совещаний сотрудников или ретритов, или сеансов планирования деятельности), а также выявлять закономерности и действия, которые следует предпринять для их устранения.

Наконец, как и все инструменты, этот инструмент можно адаптировать. Некоторым пользователям может показаться, что не все вопросы актуальны или что необходимы дополнительные вопросы. Главный принцип должен заключаться в том, чтобы собирать только ту информацию, которая может оказаться полезной, и не делать этот процесс слишком обременительным, особенно для людей, которые недавно пережили травматический опыт.

Обратите внимание, что этот журнал, скорее всего, будет содержать конфиденциальную информацию или сведения деликатного характера. Рассмотрите возможность разработки системы кодирования, чтобы избежать включения личной информации, в частности, в разделах «6. Цель» и «7. Где произошел инцидент».

Ниже показан вымышленный пример заполнения журнала инцидентов в области безопасности:

Журнал инцидентов в области безопасности — вымышленный пример			
	Вопрос	**Как ответить**	**Ответ**
1	№ инцидента	Начните с номера 1 и продолжайте по порядку; нумерация позволяет связать инциденты в области безопасности друг с другом по номерам (см. вопрос №14)	10
2	Дата происшествия	Введите ГОД-МЕСЯЦ-ДЕНЬ (например, 2019-02-17, для даты 17 февраля 2019 г.), чтобы упорядочить журнал событий безопасности по дате.	2022-11-4
3	Время происшествия	Конкретное время суток (если известно) или более общее (утро, день, вечер, ночь)	11:34
4	Виновник инцидента	Имя, если оно известно и его безопасно указать, или используйте более общий термин, например «сотрудник правоохранительных органов».	Неизвестный злоумышленник – возможно, член местной банды.
5	Пострадавшая организация	Название партнера по реализации программы по ВИЧ (т.е. название общественной организации)	Вымышленная организация
6	Цель (объект)	Конкретный человек или тип сотрудников, физическое пространство (например, название конкретного заведения), веб-сайт, база данных и т.д. Не называйте здесь имена людей, если у вас нет на это их разрешения.	Центр доверия для ключевых групп населения
7	Где произошел инцидент	Физический адрес, интернет, телефонный звонок и т.д.	Индепенденс лейн, 40, Ньютаун
8	Предполагаемый мотив нападения (если он известен)	Например: запугивание, прекращение программ, отвлечение внимания от других местных проблем	Запугать сотрудников программы и нанести ущерб помещениям, чтобы остановить оказание услуг, поскольку считалось, что это поощряет аморальное поведение.
9	Описание инцидента в области безопасности	Например: В сообщениях Facebook на странице проекта говорилось: «[вставьте сюда конкретное сообщение»]; или инструкторы, работающие по принципу "равный-равному", были арестованы без предъявления обвинений при раздаче презервативов группе MCM во время мобильного мероприятия по тестированию на ВИЧ.	Зачинщик напал на некоторых пользователей и волонтеров центра с применением силы.
10	Последствия инцидента в области безопасности для программы	Например: Партнер-исполнитель будет проводить информационно-разъяснительную работу только через Интернет до тех пор, пока очные аутрич-мероприятия не будут признаны безопасными	Центр пришлось временно закрыть, а последующие информационно-просветительские мероприятия в этом районе были отменены.
11	Описание действий, предпринятых для реагирования на инцидент в области безопасности	Например: В ГОД-МЕСЯЦ-ДЕНЬ партнер-исполнитель, ставший объектом угроз в Facebook, решил, что проводить аутрич деятельность в течение двухнедельного периода небезопасно, и партнер-исполнитель подал жалобу в полицию. Укажите даты предпринятых действий (и продолжайте обновлять эту строку по мере принятия мер)	Организация подала жалобу в полицию и местному мэру, но они не предприняли никаких действий.
12	С какими еще инцидентами в области безопасности это связано? (если таковые есть)	Отметьте, был ли этот инцидент связан с другими инцидентами в области безопасности, указав здесь номера других инцидентов.	Связан с инцидентами 2, 7 и 8.
13	Урегулирование инцидентов (если таковое имело место)	Например: В ГОД-МЕСЯЦ-ДЕНЬ инструкторы, работающие по принципу "равный-равному" были освобождены из-под стражи и им была оказана психологическая помощь.	Пока еще не урегулирован

Чтобы загрузить электронную версию этого инструмента, нажмите на ссылку далее:
В формате Word: https://www.civilsocietyhealth.Org/website/wp-content/uploads/2022/12/1.-Security-Incident-Log-Word.docx
В формате Excel: https://www.civilsocietyhealth.org/website/wp-content/uploads/2022/12/1.-Security-Incident-Log-Excel.xlsx

02 Инструмент 2: Контрольный список стратегий безопасности

Описание

Этот контрольный список предназначен для того, чтобы помочь исполнителям лучше понять, в какой области деятельности их организации уже приняты надежные меры безопасности, а где есть возможности для их дальнейшего усиления. Организации проводят самооценку того, что они в настоящее время делают, по ряду категорий. Затем инструмент позволяет создать диаграмму, которая является визуальным представлением сильных и слабых сторон организации.

Помимо использования этого инструмента для выявления собственных потребностей организации, результаты можно использовать для содействия развитию навыков взаимодействия с другими аналогичными организациями.

Периодическое использование контрольного списка может помочь организации оценить, добивается ли она прогресса в каких-либо областях или возникают ли новые проблемы, которые необходимо решить.

Как это использовать

Инструмент предоставляется в формате Excel и включает подробные инструкции по использованию, в том числе, кто и какие компоненты оценки должен выполнять. Хотя он предназначен для использования отдельными организациями, его также можно использовать в контексте совещаний или семинаров с участием нескольких организаций для облегчения взаимного обучения. Например, представители каждой организации могут провести самооценку для своей организации, после чего каждая организация может поделиться своими результатами и предоставить другим участникам дополнительную информацию о тех областях, в которых они считают себя наиболее сильными.

Чтобы загрузить электронную версию этого инструмента, нажмите на ссылку далее:

- https://www.civilsocietyhealth.org/website/wp-content/uploads/2022/12/2.-Checklist-of-Security-Strategies.xlsx

Инструмент 3: Оценка угроз, рисков и уязвимости

Описание

Для любой организации, в которой происходят инциденты в области безопасности, важно лучше понимать, почему они возникают. Журнал инцидентов в области безопасности является хорошей отправной точкой для этого, поскольку он позволяет собирать подробную информацию об угрозах или инцидентах, с которыми столкнулась организация, ее сотрудники и волонтеры. Более внимательно просматривая журнал инцидентов, сотрудники организации могут определить, что делает данную организацию или ее сотрудников уязвимыми, а также насколько серьезными являются угрозы и риски с точки зрения вероятности их материализации и их последствий. Это, в свою очередь, помогает продумать, какие меры следует принять для предотвращения инцидентов и реагирования на них. Этот инструмент предлагает некоторые вопросы, которые можно использовать для оценки угроз, рисков и уязвимости.

Как это использовать

Не существует твердо установленного формата или подхода к использованию этого инструмента. Вопросы могут использоваться менеджерами или членами команды при анализе произошедших инцидентов или в рамках планирования программы, чтобы обеспечить учет вопросов безопасности в планах действий.

Системный подход к **оценке угроз** включает в себя работу в группе с другими сотрудниками программы, чтобы ответить на следующие вопросы:

A. Каковы факты, связанные с угрозой? (Что мы на самом деле знаем об этой угрозе, а не то, что предполагаем?).

- Это полезно, потому что напоминает нам о необходимости отказаться от сплетен и домыслов. Иногда угроза может быть преувеличена или недооценена из-за того, как ее воспринимают другие. Старайтесь думать только о фактах.

B. Существует ли ряд угроз, которые со временем становятся более систематическими или частыми? (Человек угрожает каждый день или просто беспокоит, когда представляется такой случай? Усугубляются ли риски с точки зрения близости, например, когда зачинщики находят людей у них дома или на работе?).

- Если что-то происходит несколько раз, это увеличивает серьезность угрозы. Это показывает, что у человека/людей имеется определенная фиксация на мысли о создании угрозы. Эскалация угрозы — например, кто-то кричал на вас, когда вы проводили разъяснительную работу, а теперь вас также нашли в Интернете — это еще один признак того, что ситуация более серьезна.

C. Кем является человек, который угрожает? (Это кто-то известный? Тот, кто обладает способностью влиять на других? Кто-то, у кого есть информация, которая может навредить вам или вашим коллегам?)

- Этот вопрос помогает понять, какой властью обладает угрожающий человек. Например, угрожающий полицейский, скорее всего, будет более опасен, чем какой-то незнакомец.

D. Какова цель угрозы? (Чтобы изменить ваше поведение? Чтобы напугать? Это политический инструмент для получения голосов?)

- Размышление об этом может помочь вам решить, готов ли человек к эскалации конфликта. Например, если это просто для того, чтобы напугать меня, то, возможно, этот человек никогда не собирается причинять мне физический вред, даже если он говорит, что сделает это. Знание этого также может помочь вам решить, как действовать.

E. Насколько серьезной, по вашему мнению, является угроза? (Ваше личное мнение по данной теме)

- Здесь, опираясь на свою интуицию и понимание ситуации в целом, вы можете судить о серьезности угрозы. Этот анализ может проводиться на основе угроз или инцидентов, зарегистрированных в журнале безопасности организации.

На практике организация или программа могут изучить каждую угрозу или инцидент, записанные в журнале безопасности (см. Инструмент 1), и заполнить таблицу, отвечающую на каждый из приведенных выше вопросов, как показано в вымышленном примере ниже, в котором речь идет о том же инциденте, который был описан ранее.

Вопрос	Ответ (вымышленный)
Каковы факты, связанные с угрозой?	Зачинщик один вошел в центр доверия, угрожал и нападал на получателей услуг и волонтеров.
Являются ли эти угрозы частью серии угроз, которая со временем стала более систематической или частой?	Да, аналогичные попытки предпринимались и другими зачинщиками, хотя и с меньшей ожесточенностью. Все они были записаны в журнал инцидентов.
Кем являются люди, высказывавшие угрозы?	Судя по всему, они являются членами местного сообщества, живущими недалеко от центра доверия, и могут быть членами местной банды. Известно, что некоторые из них являются прихожанами церкви, в которой постоянно звучат проповеди против гомосексуализма.
Какова цель угрозы?	Чтобы предотвратить деятельность и закрыть центр.
Как вы думаете, насколько серьезна угроза?	Очень серьезна. Большую обеспокоенность вызывает угроза физическому и психическому здоровью как пользователей услуг, так и тех, кто работает в центре доверия. Мы думаем, что из-за бездействия полиции такие случаи будут повторяться.

Угрозу можно проанализировать подробнее, если более тщательно изучить характеристики зачинщика или злоумышленника. Для осуществления угрозы или акта насилия зачинщику или злоумышленнику необходимо следующее:

- **Доступ**: к потенциальной жертве или организации, физический или виртуальный. Это может означать, что они знают, где находится помещение, используемое программой, и они могут беспрепятственно проникнуть в него; или что они могут идентифицировать онлайн-работников по их аккаунтам в интернете и использовать это для совершения злонамеренных действий или кражи информации.
- **Ресурсы**: все, что может быть использовано для злонамеренных действий – например, информация о местонахождении жертвы или ее слабостях; наличие оружия, транспорта или денег, позволяющих совершить злонамеренные действия.
- **Безнаказанность**: это означает, что осуществление злонамеренных действий не влечет никаких последствий: например, никаких юридических последствий или противодействия таким действиям со стороны общества.
- **Мотив**: причина для совершения злонамеренных действий или высказывания угроз. Это может быть связано с их отношением к программе или определенной группе населения или с их предположениями в их отношении. В некоторых случаях бывает целесообразно ограничить распространение информации о том, чем мы занимаемся. В других случаях будет полезно разъяснить им, что мы делаем, потому что это приносит пользу обществу в целом. В некоторых других случаях мы можем решить, что изменение мнения других людей не является нашей целью, и тогда будет предпочтительно сосредоточиться на ограничении трех других факторов риска.

Причина рассмотрения этих четырех факторов заключается в том, что это также может помочь определить, как можно уменьшить или ослабить каждый из них. Не существует «правильных» ответов, и часто ограничение доступа для злоумышленника может также ограничить доступ для бенефициаров вашей программы (например, если вы не опубликуете адрес своей клиники в Интернете, ни злоумышленник, ни человек, желающий пройти тестирование на ВИЧ, не смогут вас легко найти). Принятие этих решений предполагает компромиссы. Опять же, для систематического анализа можно использовать таблицу, как показано ниже, используя тот же вымышленный пример, который был приведен выше.

	Что на данный момент есть у злоумышленника?	**Как ваша программа может уменьшить указанные риски?**	**Каковы компромиссы, если вы решите действовать таким образом?**
Доступ:	Злоумышленник может беспрепятственно проникнуть в центр доверия для ключевых групп населения.	Обеспечьте наличие журнала регистрации всех посетителей и их проверку/присутствие охранника.	Потребность в ресурсах для реализации некоторых мер безопасности.
Ресурсы:	Злоумышленник располагает конкретной информацией о местонахождении центра и имеет оружие.	Организация может распространять информацию о том, что центр обслуживает ключевые группы населения, в более завуалированной форме.	Настоящим пользователям услуг может быть не так легко найти клинику; некоторые могут предпочесть публичность, чтобы отстаивать свои права.
Безнаказанность:	Лидеры местных сообществ и средства массовой информации не выступают открыто против нападавшего, а полиция не проводит расследования.	Разъяснительные мероприятия, направленные на то, чтобы заинтересованные стороны поняли, что все люди имеют права; привлечь юридическую помощь для обеспечения проведения расследования и предъявления обвинений.	Требует долгосрочных усилий и приверженности, а также тщательного мониторинга ситуации.
Мотив:	Стигма и негативное отношение к ключевым группам населения; зависть к тому, что ключевые группы населения получают те или иные услуги.	Предоставлять услуги более широкому кругу населения. Работайте с местными лидерами и сообществом для улучшения отношения к КГН.	Если услуги будут доступны более широким слоям населения, некоторых пользователей услуг из числа ключевых групп населения это может вынудить отказаться от их получения.

04 Инструмент 4: Планирование мер по обеспечению безопасности

Описание

Этот инструмент обеспечивает базовую структуру, которая объединяет информацию из других инструментов (о потенциале, угрозах, рисках, уязвимостях и инцидентах) для включения ее в план, который может помочь предотвратить возникновение инцидентов и помочь программе эффективно реагировать на возникающие угрозы или инциденты.

В рамках программы для ключевых групп населения существуют разные риски или уязвимости, связанные с разными видами деятельности – например, аутрич-работа в очном и в онлайн режиме сопряжена с разными рисками; на уровень риска также влияет и место проведения работы. Если программа включает в себя такие помещения, как клиника или центр доверия, то они также могут иметь определенные уязвимости, которые необходимо устранить с помощью мер безопасности.

Многие меры безопасности включают простые изменения в способах работы организации или программы и не обязательно требуют затрат. Однако усиление безопасности может также потребовать нового оборудования, консультаций или персонала, стоимость которых необходимо будет оценить и включить в бюджет программы.

Как это использовать

Подход к планированию, рекомендуемый в этом инструменте, направлен на оценку рисков и составление плана действий по *каждому* виду деятельности, осуществляемому в рамках программы. Результатом планирования мер в области безопасности является не один план по обеспечению безопасности для всей программы или организации, а скорее набор конкретных планов безопасности, каждый из которых связан с каждым видом деятельности, которым занимается программа, или с риском, с которым она сталкивается.

Поскольку планирование мер в области безопасности должно быть неотъемлемой частью планирования деятельности или работы, а не отдельным процессом, рекомендуется использовать этот инструмент планирования мер в области безопасности каждый раз, когда разрабатываются или пересматриваются планы деятельности. Информация из журнала инцидентов, контрольного списка стратегий безопасности и анализа угроз должна учитываться и использоваться в рамках этого процесса.

В данный процесс должны быть вовлечены лица, участвующие в реализации каждого вида деятельности, которые должны принимать участие в выявлении рисков безопасности и согласовании соответствующих мер в области безопасности. Поскольку риски в области безопасности могут меняться со временем, планы по обеспечению безопасности для каждого вида деятельности также следует периодически обновлять, особенно когда известно, что ситуация изменилась.

Планирование мер по обеспечению безопасности включает в себя составление плана по снижению рисков причинения вреда исполнителям, связанных с любой конкретной деятельностью. В то же время это, вероятно, принесет пользу бенефициарам и сообществу в целом. Поэтому этот инструмент следует использовать для планирования обеспечения безопасности в отношении каждого вида деятельности организации или программы и каждой из наиболее важных проблем безопасности, связанных с этой деятельностью.

Для каждого центра доверия, каждого аутрич-мероприятия или места его проведения потребуется отдельный план (причем для аутрич-работы в очном и онлайн режимах потребуются разные планы) и т.д.

Эти планы также следует пересматривать с течением времени. Предлагается делать это во время регулярных

совещаний программной группы/ совещаний по планированию, чтобы это стало составной частью планирования, а не отдельным видом деятельности.

Планы обеспечения безопасности должны учитывать информацию и аналитические данные, собранные с помощью инструментов 1, 2 и 3. Планы могут иметь форму простой таблицы – вот пример заполненной таблицы рисков, с которыми можно столкнуться во время аутрич-работы с ключевыми группами населения в барах:

План обеспечения безопасности для:		**Аутрич-работы, проводимой в барах инструкторами по принципу "равный-равному" для секс-работников**	
Дата пересмотра плана обеспечения безопасности:	**Дата разработки/последних изменений**	**1/1/2020**	
Ответственное лицо:		**Менеджер**	
Риск, который необходимо устранить:		**Риск физического нападения на аутрич-работников во время аутрич-мероприятий в барах**	
Угрозы	**Факторы уязвимости**	**Имеющийся потенциал**	**Необходимый потенциал**
Словесные оскорбления, включая угрозы физического насилия, имели место с момента начала проекта и в последнее время усилились; зачинщиками часто являются владельцы баров, которые не хотят, чтобы в их заведениях проводилась аутрич-работа.	Аутрич-работу проводят секс-работники, которые вряд ли сообщат о неправомерных действиях; информационно-пропагандистская (аутрич-) работа проводится регулярно в ночное время; работники транспортом не пользуются; приходят пешком; владельцы баров не хотят, чтобы аутрич-работники поощряли секс-работников использовать презервативы, потому что они считают, что в результате клиенты будут платить меньше	Аутрич-работники, работающие по принципу «равный равному», носят удостоверения личности, на которых указано, что они связаны с Министерством здравоохранения, а также имеется номер телефона, по которому можно связаться с местным офицером полиции, прошедшим соответствующее обучение; аутрич-работники работают в парах; аутрич-работники имеют телефоны с предоплаченным трафиком для связи в случае чрезвычайной ситуации; аутрич-работников обучают тому, как описывать свою работу, не вызывая негативной реакции; их местонахождение отслеживается с помощью регистрационного журнала; у них есть безопасные убежища в каждом районе, где они работают, поскольку секс-работники их знают и уважают.	В дополнение к имеющемуся потенциалу, начать разъяснительную работу с владельцами баров, чтобы уменьшить оскорбительное поведение с их стороны. Если риски для аутрич-работнико в остаются высокими, перенесите деятельность в другие места, где собираются секс-работники.

Хотя для каждого вида деятельности требуется собственный план обеспечения безопасности, весьма вероятно, что разные планы будут включать схожие меры. Поэтому менеджерам программ следует проанализировать все планы и определить, можно ли принять некоторые меры совместно, например, в отношении обучения персонала или партнеров или приобретения оборудования, которое можно использовать для повышения безопасности всех видов деятельности.

Рассмотрите также возможность разработки в приоритетном порядке планов безопасности для наиболее серьезных угроз, с которыми сталкивается ваша программа.

Инструмент 5: Практические советы по включению мер обеспечения безопасности программ в гранты Глобального фонда

Описание

Хотя меры безопасности сильно зависят от конкретной ситуации и не могут быть едиными для всех, опыт показывает, что полезно предложить определенные типы действий, которые можно запланировать, и описать, как они могут быть включены в гранты Глобального фонда, особенно если они предполагают затраты. В этом инструменте представлены некоторые основные идеи и несколько советов о том, как включить их в планы по реализации грантов.

Как это использовать

В отличие от других инструментов, это не контрольный список или конкретное мероприятие, а скорее набор предложений, которые пользователи могут рассмотреть. Не рекомендуется автоматически включать все мероприятия в план программы; скорее, исполнителям следует подумать, будут ли какие-либо из этих мероприятий полезны для повышения безопасности их программ.

Основные меры безопасности

Хотя проблемы безопасности, с которыми сталкивается каждая организация и программа, различны, и эти проблемы меняются со временем, опыт показывает, что существуют некоторые основные виды деятельности и практики, которые актуальны для большинства программ. Рассмотрение их актуальности для вашей программы может стать хорошим способом подумать о том, как улучшить вашу безопасность.

A. Вопросы безопасности должны стать стандартной частью вашей программы — проверяйте все запланированные мероприятия на предмет потенциальных угроз безопасности, при необходимости принимая меры по смягчению последствий и реагированию. Идеи по смягчению последствий или реагированию могут включать следующее:
Предоставьте всем сотрудникам и волонтерам удостоверения личности с указанием их имени, организации, должности и контактных данных их организации или руководителя.

- Разработайте соглашение с юристом (например, договор о представлении им интересов вашей организации), который сможет оказать правовую поддержку в случае возникновения инцидентов.
- Укажите на хранящейся должным образом карте (которая не должна содержать информации, которую могли бы идентифицировать другие) места, охваченные программой, в том числе те, которые являются более безопасными/рискованными, а также информацию о том, как получить к ним доступ. Также обратите внимание на наличие в каждом месте союзников/коллег (например, полиции, медицинских работников, общественных лидеров), которые могут помочь в случае чрезвычайной ситуации.
- Инвестируйте в инфраструктуру безопасности, такую как замки и решетки на окнах, в офисах и центрах доверия.
- Пусть аутрич-работники работают как минимум парами. Разработайте процедуры регистрации убытия/прибытия для аутрич-работников и других полевых команд, а также обеспечьте безопасную транспортировку к местам аутрич-работы и обратно.
- Используйте журналы регистрации посетителей, чтобы записывать, кто выходит и входит в учреждение или пункт доверия.

B. Обсуждайте инциденты и проблемы безопасности на регулярных совещаниях членов команды (не реже

одного раза в месяц) и призывайте всех сотрудников и волонтеров делиться проблемами и опасениями, связанными с безопасностью. Записывайте все инциденты, угрозы и предпринятые действия в журнале и периодически просматривайте эти записи, чтобы выявить тенденции и внести изменения в планы действий (например, если вы определите конкретные горячие точки, которые все чаще представляют опасность, обеспечьте ротацию сотрудников или усиливайте меры безопасности в горячих точках).

C. Проведите обучение всех работников (включая персонал и волонтеров) мерам по обеспечению безопасности при реализации программы. Это должно включать в себя выявление и оценку угроз, а также ожиданий каждого работника в случае возникновения угрозы (например: Что им следует сделать, чтобы избежать вреда? К кому им следует обратиться за помощью в случае причинения им вреда? Какие действия, например немедленное прекращение аутрич-деятельности, они имеют право предпринять самостоятельно? Какая меры защиты предусмотрены для них, если они получили травму на работе или стали жертвами кражи или других преступлений?). Нет необходимости организовывать специальный тренинг по безопасности — вы можете сделать это, включив вопросы безопасности во все тренинги, связанные с программой, в том числе в тренинги по принципу "равный-равному" и тренинги для поставщиков медицинских услуг.

D. Имейте план быстрого реагирования на случай чрезвычайных ситуаций и кризисов, включая четкие каналы связи, четкие процессы принятия решений и гибкое финансирование, к которому можно легко получить доступ.

E. Назначьте ответственного за безопасность в организации — это может быть человек с существующими обязанностями по управлению или координации. Его роль будет заключаться в том, чтобы объяснять и напоминать коллегам о действующих принципах и процедурах. Этот человек должен пройти обучение и действовать под контролем другого сотрудника.

F. Определите союзников, которые могут оказать поддержку в случае инцидентов и держите их в курсе любых изменений ситуации с безопасностью (поддерживая четкие каналы связи, установленные до того, как инциденты произойдут).

G. Разработайте телефонное дерево/группу экстренной связи для всех сотрудников и волонтеров, чтобы каждый знал, к кому обращаться в той или иной ситуации и как передавать срочные новости в случае возникновения чрезвычайной ситуации.

H. Сотрудники и волонтеры должны тщательно обдумать и решить, какую информацию публиковать (например, местонахождение учреждения или свою личную информацию в случае инструкторов, работающих онлайн по принципу "равный-равному), взвесив все «за» и «против» публикации такой информации

Включение мер по обеспечению безопасности в запросы на финансирование Глобального фонда

A. Решение о том, как интегрировать мероприятия по обеспечению безопасности в запрос

Не все мероприятия по обеспечению безопасности требуют финансирования или определенной статьи бюджета. Например, обеспечение того, чтобы вопросы безопасности включались в повестку дня всех совещаний специалистов по реализации или планированию, скорее всего, не повлечет за собой никаких затрат, поскольку эти совещания и так уже проводятся. Другие виды деятельности, такие как включение процедур безопасности в тренинги для членов команды, а также открытие журнала регистрации посетителей и журнала инцидентов в области безопасности, могут потребовать некоторого увеличения существующих бюджетов (например, стоимость продления тренинга на полдня). В этих случаях подход должен заключаться в обеспечении того, чтобы бюджеты на существующие мероприятия были достаточными для покрытия любых дополнительных мер, связанных с безопасностью.

В некоторых случаях повышение безопасности потребует особых инвестиций в дополнительные мероприятия

или оборудование. Примеры включают наем консультантов и закупку оборудование для улучшения хранения цифровой информации, меры физической безопасности (например, замки, сигнализация, камеры) или новый персонал (охранники). Затраты также могут быть связаны с дополнительными совещаниями с заинтересованными сторонами, направленными на повышение безопасности. Другим примером являются фонды непредвиденных расходов или быстрого реагирования, которые можно использовать для поддержки сотрудников или волонтеров, пострадавших в результате инцидента в сфере безопасности.

B. Приемлемость расходов, связанных с безопасностью

Все эти расходы могут финансироваться в рамках грантов Глобального фонда, как указано в соответствующих материалах запроса на финансирование (например, в Информационных бюллетенях, технических записках и модульной структуре)[1]. Как и в случае с любым финансированием, запрашиваемым в Глобальном фонде, важно, чтобы они были оправданы и основывались на подтвержденных потребностях. (И здесь очень полезным будет использование самооценки стратегий безопасности, журнала инцидентов и инструментов планирования). Форму запроса на финансирование следует использовать для разъяснения проблем в сфере безопасности, с которыми сталкивается или может столкнуться проект, а также того, как эти проблемы будут решаться посредством предлагаемых мероприятий и статьи бюджета.

Важным элементом безопасности программы является способность реагировать при возникновении инцидента, чтобы оказать немедленную помощь пострадавшим работникам программы – это может включать экстренное предоставление жилья, эвакуацию, медицинскую помощь или юридическую помощь. Как и в случае любой деятельности, предлагаемой для финансирования Глобальным фондом, для включения статьи бюджета на создание такого фонда в запрос на финансирование необходимо продемонстрировать, что это является необходимым, разумным и будет способствовать прямо или косвенно достижению целей программы. Поэтому включение в запросы на финансирование доказательств возникновения инцидентов и угроз в прошлом, а также их влияния на программу, будет иметь важное значение. Использование фондов на непредвиденные расходы должно будет осуществляться в соответствии с применимыми законами и правилами, а также потребуются прозрачные и справедливые критерии и условия для их распределения среди бенефициаров.

C. В какой раздел бюджета Глобального фонда могут быть включены расходы на безопасность

Что касается включения расходов на безопасность в бюджет Глобального фонда, оптимальным подходом является их интеграция в программный модуль, с которым они непосредственно связаны, а не представление мер безопасности в качестве отдельной программы или области работ. Например, если меры безопасности связаны с реализацией программы поддержки МСМ, их следует включить в качестве вмешательств в модуль ВИЧ/МСМ. Если они связаны с защитой людей, участвующих в программах по правам человека, они должны быть включены в модуль «Права человека». Многие организации-исполнители работают с разными ключевыми группами населения и одновременно осуществляют правозащитную деятельность. В таких случаях вместо того, чтобы разделять затраты на мероприятия по обеспечению безопасности, которые актуальны для всех этих программных областей, имеет смысл включить их в одно место, например, в раздел «Укрепление систем сообществ – усиление организационного потенциала».

D. Финансирование расходов, связанных с безопасностью, обеспечивается исполнителям, работающим непосредственно с бенефициарами.

Многие программы по ВИЧ для ключевых групп населения получают финансирование от Глобального фонда для борьбы со СПИДом, туберкулезом и малярией. По большей части это финансирование поступает не напрямую организациям, работающим с КГН, а через основного получателя (ОП), у которого есть грантовое соглашение с Глобальным фондом, а иногда и через субполучателей (СП), с которыми ОП заключил договор.

В каждой стране Страновой координационный механизм (СКМ) несет основную ответственность за разработку запросов на финансирование, а ОП играют ведущую роль в разработке подробных рабочих планов и бюджетов и в реализации грантов. Поэтому важно, чтобы СКМ и исполнители понимали проблемы безопасности, с которыми сталкиваются программы для ключевых групп населения, и предусмотрели любые расходы, связанные с повышением безопасности программ, при разработке запросов на финансирование и подробных бюджетов. После того, как эти расходы будут включены в бюджеты грантов, также крайне важно, чтобы эти статьи были включены в субгранты или субконтракты ОП и СП на программы для ключевых групп населения.

СКМ должны обеспечить правильное понимание потребностей в области безопасности программ по ВИЧ для ключевых групп населения на момент разработки запроса на финансирование – например, обеспечив применение действующими исполнителями инструментов настоящего пакета для регистрации инцидентов, оценки возможностей, выявления рисков и составления планов безопасности. Эта информация должна учитываться при разработке программы и гарантировать, что сметы на реализацию программы отражают любые затраты, связанные с безопасностью.

[1] https://www.theglobalfund.org/en/applying-for-funding/design-and-submit-funding-requests/applicant-guidance-materials/