Image not found or type unknown

Оценка Рисков

Ознакомьте участников с концепциями, лежащими в основе оценки рисков, и с тем, как применять рамки оценки рисков для обеспечения личной и/или организационной безопасности **Настоятельно рекомендуем** выбрать Путь обучения для планирования, поскольку он содержит упражнения с разным уровнем глубины, которые помогут участникам_цам получить более глубокое представление об изучаемых предметах.

- Направления обучения & Обучающие упражнения
- Упражнение: введение в оценку рисков [Разминочное упражнение]
- Оценка коммуникативных практик [Разминочное Упражнение]
- Ежедневная Круговая Диаграмма и Риск [Разминочное Упражнение]
- Улица ночью [Разминочное упражнение]
- Переосмысление риска и пять слоев риска [Углубленное Упражнение]
- Упражнение: «Жизненный цикл данных как способ понимания риска» [Углубленное упражнение]
- Организация протестов и оценка рисков [Тактическое Упражнение]
- Основы оценки рисков [Базисный материал]
- Оценка рисков при формировании движения [Базисный материал]

Направления обучения & Обучающие упражнения

> **На этой странице** вы найдете руководство по правильному использованию и пониманию Модуля. Следование Путям обучения, включающим упражнения различной глубины, должно позволить участникам лучше усвоить изучаемые темы.

risk_assessment_RUSSIAN.png
Image not found or type unknown

Картинка с изображением. Водопад, в котором купаются люди, На берегу дерево с качелью и человеком. Силет ходит по канатке.

Цели обучения

К концу этого модуля участники_цы смогут:

- Понимать концепции, которые лежат в основе оценки рисков
- Применять механизмы по оценке рисков для обеспечения личной и/или организационной безопасности
- Разработать собственный метод проведения оценки рисков, который будет соответствовать их потребностям

Обучающие упражнения

Разминочные упражнения

image_1605640724450.png
Image not found or type unknown

- Упражнение: введение в оценку рисков
- Оценка коммуникативных практик

- Ежедневная Круговая Диаграмма и Риск
- Разминочное упражнение: «Улица ночью»

Углубленные упражнения

image_1605640735000.png
Image not found or type unknown

- Переосмысление риска и пять слоев риска
- Углубленное упражнение: «Жизненный цикл данных как способ понимания риска»

Тактические упражнения

image_1605640743110.png
Image not found or type unknown

- Тактическое упражнение: «Организация протестов и оценка рисков»

Базисные материалы

- Основы оценки рисков
- Оценка рисков при формировании движения

*Картинка с рисунком. На рисунке растения синего цвета

image_1605452256072.png
Image not found or type unknown

Упражнение: введение в оценку рисков [Разминочное упражнение]

Image not found or type unknown starter_activ_circular_400px-with-text_russian.png

Картинка. Надпись на картинке: Разминочные Упражнения

Рисунок на картинке: темно-синий круг. В центре круга желтый водоросль с корнями

Это упражнение предназначено для ознакомления и отработки основ оценки рисков.

Цели обучения

Цели обучения данного упражнения отвечают следующим задачам

- Понимать концепции, лежащие в основе оценки рисков
- Приступить к применению системы оценки рисков для обеспечения личной и/или организационной безопасности.

Для кого предназначено данное упражнение?

Данное упражнение предназначено для участников_ц, имеющих базовый опыт оценки рисков или не имеющих его вовсе. Он также предназначен для семинара с участниками_цами из разных организаций.

Продолжительность

Если быть реалистичными, для правильного проведения упражнения потребуется день (как минимум 8 часов)..

Ресурсы, Необходимые для данного упражнения

- Бумага для флипчарта + маркеры
- Проектор
- Ноутбуки

Техника проведения

Для этого упражнения сочините историю о человеке или группе, на примере которых участники_**цы** смогут попрактиковаться в проведении оценки риска.

В зависимости от состава участников_ц, возможны следующие варианты:

- группа по правам человека в стране, которая только что приняла закон о контроле за НПО

- транс-женщина, запускающая веб-сайт для поддержки других транс-женщин
- сеть защитниц прав женщин, работающих над проблемой, которая считается запретной в их странах
- группа с убежищем для молодых транс-людей
- небольшая группа ЛГБТИК, подвергающаяся нападкам в интернете
- квир-женщина из группы расовых меньшинств, размещающая свое мнение в интернете.

Разделите участников_ц на группы. Они могут работать над одной и той же организацией/группой или над разными организациями.

> **Примечание по фасилитации:** важно, чтобы история резонировала с участниками_цами и была близка их опыту.

Как только все участники разойдутся по группам, презентуйте **тему «Основы оценки рисков»**, Презентация по оценке рисков.

Работа в группах 1: разработка контекста и сценария

Прежде чем группы начнут заполнять шаблон "Оценки риска", они должны проработать выбранный ими сценарий истории Шаблон Оценки Рисков

Для сценария истории группы:

- Создайте профиль этой организации - местоположение, размер организации, общая миссия организации
- Перечислите ее виды деятельности или изменения в контексте, которые подвергают организацию риску (это может быть новый закон, или группа планирует действия, которые недоброжелатели захотят прервать. Это также могут быть внутренние изменения, которые могут представлять риск - например, недавний конфликт внутри организации или внешнее событие, которое вызывает значительный внутренний стресс среди членов организации)

- Назовите, кто будет настроен враждебно по отношению к действиям группы, и кто является их союзниками.

Создайте профиль этого человека - возраст, местонахождение, сексуальная ориентация, насколько он_а активен_на в социальных сетях

- Создайте мнение, за которое человек подвергается нападкам. Или опишите созданный им сайт, который подвергает его риску. Или контекст, который создает уязвимую ситуацию (например, человека выгнали из дома, он разорвал абьюзивные отношения с кем-то из той же организации или движения и т.д.).
- Назовите, кто будет настроен враждебно по отношению к его действиям, и кто является его союзниками.

Дайте каждой группе час на выполнение этого задания.

После этого попросите каждую группу быстро представить свои сценарии.

Затем представьте **шаблон оценки рисков**. Risk assessment template.

Примечания к таблице:

- Угрозы должны быть **конкретными** – в чем заключается угроза (негативное намерение по отношению к человеку / группе) и кто угрожает?
- Подумайте о **вероятности** угрозы с трех сторон:
  - Уязвимость – какие процессы, действия и поведение человека или группы увеличивают вероятность того, что угроза станет реальной?
  - Возможности людей/лиц, осуществляющих угрозу - кто угрожает и что они могут сделать для осуществления угрозы?
  - Известные инциденты - поступала ли подобная угроза в аналогичной ситуации? Если ответ положительный, то вероятность возрастает.
- Размышляя о **воздействии**, учитывайте не только индивидуальное воздействие, но и на сообщество в целом.
- Оценка низкой /средней /высокой вероятности и воздействия всегда будет относительной. Но важно провести эту оценку, чтобы определить приоритетность рисков, для которых необходимо разработать планы по снижению воздействия.
- Риск — это формулировка, содержащая угрозу и вероятность ее возникновения.

Работа в группах 2: оценка рисков

С помощью шаблона "Оценка рисков" каждая группа анализирует риски в своем сценарии. Задача состоит в том, чтобы определить различные риски и проанализировать каждый из них.

> **Примечание по фасилитации:** раздайте каждой группе электронную копию шаблона оценки рисков, чтобы они могли документировать свои обсуждения непосредственно в ней.

После окончания подведите итоги вместе с группами, но сделайте это, не требуя от них отчетов по шаблонам. Задавайте вопросы о самом процессе:

- Какие трудности возникли у вашей группы при оценке рисков?
- Какие основные угрозы вы выявили?
- Какие вызовы возникли при анализе вероятности?

Вводная информация и обсуждение тактик смягчения последствий

Используя текст для презентации по тактикам смягчения последствий (см. раздел "Презентация"), представьте основные аспекты и проведите обсуждение с участниками_цами.

Работа в группах 3: планирование мер по смягчению последствий

Попросите каждую группу определить риск с высокой вероятностью и высоким воздействием. Затем попросите их составить план по снижению этого риска.

Наводящие вопросы

Превентивные стратегии (стратегии по предотвращению)

- Какие меры и возможности у вас уже есть для предотвращения этой угрозы?
- Какие действия вы предпримете, чтобы избежать воплощения этой угрозы в жизнь? Как вы измените процессы в сети, чтобы предотвратить осуществление этой угрозы?
- Существуют ли политики и процедуры, которые необходимо создать для решения этой задачи?
- Какими навыками вы должны обладать, чтобы предотвратить эту угрозу?

Ответ на инцидент

- Как вы поступите, если эта угроза осуществится? Какие шаги вы предпримете в случае наступления этой угрозы?
- Как вы сможете свести к минимуму серьезность последствий этой угрозы?
- Какими навыками вы должны обладать, чтобы предпринять шаги, необходимые для реагирования на эту угрозу?

На эту групповую работу уйдет от 45 минут до часа.

После завершения подведите итоги, задав вопросы о процессе и о проделанной работе.

Чтобы подвести итог этого обучающего упражнения, повторим некоторые уроки:

- Оценка риска полезна для выработки реалистичных стратегий (превентивных и ответных)
- Сосредоточьтесь на угрозах с высокой вероятностью осуществления, а также на угрозах с высоким уровнем воздействия.
- Оценка риска требует практики.

Презентация

В этом упражнении необходимо представить три темы:

- Презентация по основам оценки рисков
- Шаблон оценки риска
- Материалы по тактике смягчения последствий (см. текст ниже)

Текст для презентации по тактикам снижения рисков

Существует пять основных способов снижения рисков:

Признать риск и составить планы на случай непредвиденных обстоятельств

Планирование на случай непредвиденных обстоятельств — это умение представить себе риск и наихудшее воздействие, и предпринять меры по их устранению.

Избежать риска

Уменьшите свою степень уязвимости. Какие навыки вам понадобятся? Как вам придется изменить поведение, чтобы избежать риска?

Контролировать риск

Снижайте тяжесть воздействия. Сосредоточьтесь на воздействии, а не на угрозе, и работайте над тем, чтобы свести его к минимуму. Какие навыки вам понадобятся, чтобы принять меры в отношении воздействия?

Перенаправление риска

Привлеките сторонний ресурс, который сможет взять на себя риск и его воздействие.

Мониторинг риска на предмет изменений в вероятности и воздействии

Обычно это относится к рискам с низкой вероятностью.

Существует два способа работы с рисками

Превентивные стратегии (стратегии по предотвращению)

- Какие меры и возможности у вас уже есть для предотвращения этой угрозы?
- Какие действия вы предпримете, чтобы избежать воплощения этой угрозы в жизнь? Как вы измените процессы в сети, чтобы предотвратить осуществление этой угрозы?
- Существуют ли политики и процедуры, которые необходимо создать для решения этой задачи?

- Какими навыками вы должны обладать, чтобы предотвратить эту угрозу?

Ответ на инцидент

- Как вы поступите, если эта угроза осуществится? Какие шаги вы предпримете в случае наступления этой угрозы?
- Как вы сможете свести к минимуму серьезность воздействия этой угрозы?
- Какими навыками вы должны обладать, чтобы предпринять шаги, необходимые для реагирования на эту угрозу?

Корректировка для организационного семинара

Это упражнение можно использовать в контексте семинара, когда оценка рисков проводится организацией, а роль тренера_ки-фасилитатора_ки заключается в том, чтобы провести организацию через этот процесс.

Для этого вместо детализации сценария проведите обсуждение основных угроз, с которыми сталкивается организация. Это могут быть изменения в законодательстве или правительстве, которые влияют на способность организации продолжать свою работу. Это также может быть конкретный инцидент, когда люди в организации почувствовали, что они находятся в опасности (например, партнерская организация обнаружила, что за ними следят, или сама организация оказалась под наблюдением). После этого обсудите, какими возможностями уже обладает организация - ресурсами, связями, сторонниками и союзниками, а также навыками. Обоснование деятельности по оценке рисков через построение общего знания об угрозах, с которыми сталкивается организация, и ее возможностях будет важным для остальной части процесса.

Разделите участников_ц на команды и группы, когда они будут выполнять шаблон оценки рисков.

В данном контексте планирование смягчения последствий так же важно, как и шаблон оценки рисков. Поэтому обеим разделам должно быть уделено равное время.

В организационном контексте эта работа может занять до двух дней, в зависимости от размера организации и ее деятельности.

Дополнительная литература (по желанию)

- Фундаментальные документы по ОР (оценке рисков)
- Оценка рисков при формировании движения

*Картинка с рисунком. На рисунке растения болотного цвета.

image-1605451879726.png

Image not found or type unknown

Оценка коммуникативных практик [Разминочное Упражнение]

starter_activ_circular_400px-with-text_russian.png


Картинка. Надпись на картинке: Разминочные Упражнения
Рисунок на картинке: темно-синий круг. В центре круга желтый водоросль с корнями

Это упражнение создано для того, чтобы участники_цы могли проанализировать свою практику общения (темы на которые они общаются, с кем они общаются, их каналы общения) и оценить, в чем заключаются их риски).

Данное упражнение разработано как диагностический инструмент, который можно использовать для определения приоритетности тем тренинга и/или для использования

участниками_цами при оценке своей практики общения.

Цели обучения, которым отвечает данное упражнение

Это упражнение касается понимания концепций, которые лежат в основе оценки рисков.

Для кого предназначено данное упражнение?

Данное упражнение можно проводить с участниками_цами, у которых начальный или средний уровень знаний/подготовки.

Продолжительность

Вступление к упражнению: 15 минут

Индивидуальное время проведения оценки: 15 минут

Работа в группах: 30 минут

Подведение итогов пленума: 30 минут

Всего: 1.5 часа

Ресурсы, необходимые для данного упражнения

- Электронные копии таблицы. Или печатные копии данной таблицы

- ◦ Версия для печати (.pdf)
  ◦ Редактируемая версия (.dot)

Техника Проведения

Попросите участников_иц заполнить приведенную ниже таблицу.

Тема Общения	С кем вы общаетесь на эту тему	Является ли тема конфиденциальной? (да/нет)	Для кого вы станете целью в рамках этой коммуникации?	Кана коммуни
		(Да/Нет?)		
		(Да/Нет?)		
		(Да/Нет?)		
		(Да/Нет?)		
		(Да/Нет?)		

После того как каждый_ая участник_ца заполнит свою таблицу, попросите их поделиться своими результатами друг с другом в группах.

По завершении групповой работы попросите каждую группу обсудить следующие вопросы с большой группой:

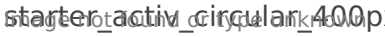
- Какие из обсуждаемых вами тем являются конфиденциальными?
- Кто те группы / сообщества / отдельные лица которые будут атаковать вас за ваше конфиденциальное общение?
- Какой коммуникационный канал вы используете чаще всего? Считаете ли вы его безопасным и конфиденциальным?

Данное упражнение может быть использовано для определения приоритетов, на каких каналов коммуникации следует сосредоточиться в оставшуюся часть семинара, или для представления альтернатив менее конфиденциальным коммуникационным каналам.

*Картинка с рисунком. На рисунке растения болотного цвета.

image_1605451879726.png

Ежедневная Круговая Диаграмма и Риск [Разминочное Упражнение]

starter_activ_circular_400px-with-text_russian.png


Картинка. Надпись на картинке: Разминочные Упражнения
Рисунок на картинке: темно-синий круг. В центре круга желтый водоросль с корнями

Целью этого упражнения является оценка участниками_цами ежедневных или еженедельных задач и анализ траты рабочего времени на выполнение каждой из них. Упражнение состоит из двух частей: создание круговых диаграмм своих еженедельных или ежедневных задач, которое заканчивается небольшой сессией обмена результатами. И вторая часть - выяснить, где в своих задачах они чувствуют себя наиболее подверженными риску. Важно, чтобы фасилитатор_ка не поднимал_а идею риска до второй части работы.

Это очень базовый способ оценки риска, который фокусируется на задачах, которые они выполняют, и на известных рисках, с которыми они обычно сталкиваются во время работы. Это занятие следует проводить вместе с более глубоким упражнением по оценке рисков.

Цели обучения, которым отвечает данное упражнение

- Применение структуры оценки рисков для своей личной и/или организационной безопасности

Для кого предназначено данное упражнение?

- Для участников_ц, не проводивших оценку рисков.
- Упражнение хорошо подходит группам, которые занимаются практически одними и теми же делами в течение всего рабочего дня.
- Это упражнение можно использовать в качестве разминочного упражнения для организации, которая собирается провести оценку организационных рисков.

Продолжительность

Минимум 1.5 часа

Ресурсы, необходимые для данного упражнения

- Бумага для флипчарта + маркеры

Техника Проведения

Первая Часть: Нарисуйте свою круговую диаграмму

Каждому участнику выдается по листу бумаги, на котором нужно нарисовать круг и разделить его на ежедневные или еженедельные задачи в организации. Деления должны отражать время, которое они уделяют каждой задаче.

Для фасилитатора_ки: Обратитесь к участникам_цам с просьбой быть как можно более конкретными в перечислении своих задач.

По завершении рисования группа собирается вместе и обсуждает следующие вопросы:

1. На выполнение каких задач каждый из них уделяет наибольшее время?
2. Какие задачи являются общими для разных участников_ц?
3. На выполнение каких задач, которым они уделяют меньше времени, они хотели бы уделять больше времени? И почему?

В частности, проведите открытую дискуссию с целью проработки их круговых диаграмм.

Вторая Часть: Определение рисков связанных с работой

Попросите участников поразмышлять над своими круговыми диаграммами и ответить на следующие вопросы:

1. Из всех задач, которые вы выполняете для своей организации, какая, по вашему мнению, связана с наибольшим риском? Каким именно риском? И почему?
2. Как вы справляетесь с рисками, связанными с этой задачей? Опишите свои стратегии.

Затем вернитесь к большой группе и проведите обсуждение.

*Картинка с рисунком. На рисунке растения синего цвета.

image-1605452256072.png

Image not found or type unknown

Улица ночью [Разминочное упражнение]

starter_activ_circular_400px-with-text_russian.png

Image not found or type unknown

Картинка. Надпись на картинке: Разминочные Упражнения
Рисунок на картинке: темно-синий круг. В центре круга желтый водоросль с корнями

Цель этого упражнения - показать, как мы на практике оцениваем риски, необходимые для жизни и выживания. В ходе выполнения этого упражнения участникам_цам будет показана темная улица ночью, чтобы они смогли ответить на вопрос: ¨Что бы вы предприняли для безопасного передвижения по этой улице в одиночку?¨

Упражнение призвано выявить способы, которыми мы автоматически оцениваем угрозы и нейтрализуем их в данной конкретной ситуации.

Цели обучения

В конце этого упражнения участники_цы:

- начнут понимать, что оценка риска не является несвойственным нам занятием
- поделятся опытом того, на что они обращают внимание при рассмотрении рискованной ситуации.

Для кого предназначено данное упражнение?

Это упражнение можно проводить с участниками_цами, которые не имеют опыта в оценке рисков, а также с теми, кто проводили оценку рисков в прошлом.

> **Примечание для фасилитатора_ки:** важно, чтобы тренер_ка-фасилитатор_ка хорошо знал_а группу, так как данное упражнение может активизировать прошлые травмы участников_ц, связанные с передвижением по ночным улицам.

Продолжительность

45 минут

Ресурсы

- Проектор, с помощью которого можно показать фотографию ночной улицы
- Доска или бумага для флипчарта, чтобы записывать ответы
- Маркеры.

Техника проведения

Ознакомьте участников_ц с упражнением, показав фотографию улицы в ночное время. Полезно также напомнить участникам_цам, что здесь нет правильных или неправильных ответов.

Ниже приведены примеры, но вы также можете выбрать собственную фотографию, которая впишется в ваш контекст.

station_at_night.jpg
Image not found or type unknown

Фотография: маленький вокзал ночью (авт. Юма Янагисава фото с платформы Flickr).

street_at_night.jpg
Image not found or type unknown

Фотография: Энди Вортингтон, ул. Дептфорд Хай ночью, фото с платформы Flickr

Дайте участникам_цам время подумать над ответом на следующий вопрос: **”Как бы вы смогли ориентироваться на этой улице в одиночку ночью?”**

> **Примечание по интерсекциональности:** не стоит полагать, что у всех участников_ц одинаковые физические возможности и способности. Именно поэтому мы используем "ориентироваться" вместо "ходить".

Попросите их самостоятельно записывать свои ответы.

На это должно уйти не более пяти минут. Не стоит заставлять участников_ц слишком долго обдумывать свои ответы.

Затем уделите некоторое время тому, чтобы участники_цы по очереди ответили на вопрос. В этот момент вы, как фасилитатор_ка-тренер_ка, просто записываете ответы участников_ц на доске или на флипчарте по мере того, как они их озвучивают.

Как только вы увидите некоторые тенденции в их ответах – как общих, так и уникальных **– начните выяснять у участников_ц причину, по которой они ответили именно так.**

На данном этапе мы в некотором роде осуществляем обратную разработку процесса. Мы начали с "как", теперь переходим к "почему". Здесь мы ищем угрозы - причины опасности, - которые они предположили в своих ответах на вопросы "как".

Записывайте и угрозы.

Хорошо бы еще раз посмотреть на фотографию, чтобы увидеть на ней элементы, которые могут представлять угрозу или возможность более безопасного ориентирования для человека, который идет по улице в одиночку.

Например, на 1-й фотографии:

- Отметьте заборы и низкий кустарник. Являются ли они хорошими укрытиями?
- По какой стороне дороги вы бы шли и почему?
- Учитывая, что это дорога, на которой находится небольшой вокзал, означает ли это, что идущему по ней человеку будет к кому обратиться, если что-то случится? Если да, то делает ли это передвижение по данной улице более безопасным?
- А как насчет того, чтобы передвигаться по этой дороге, будучи в безопасности от проезжающих мимо машин?

На 2-й фотографии:

- По какой стороне улицы вы бы шли и почему?
- Отметьте двух людей на улице - делает ли их присутствие улицу более безопасной или нет?
- Фургон дальше по улице - может ли он быть возможной причиной уязвимости или источником поддержки, если что-то случится?

Если вы планируете сделать собственную фотографию ночной улицы, продумайте наличие на ней следующих элементов:

- Вы можете сделать снимок, на котором ясно видно, где на улице расположен источник света, и при этом хорошо видна темная сторона улицы.
- Вы можете сделать снимок, где на улице будут наличествовать элементы, добавляющие больше риска. Например, мест, где кто-то может спрятаться от идущего человека. Или улицы с интенсивным автомобильным движением.

Обсудив с участниками_цами тактику безопасности и угрозы, задайте им вопрос: ¨**Что еще нужно знать об этой улице, чтобы принимать более правильные решения о безопасной навигации по ней?**¨

Дайте время участникам_цам обдумать свои ответы.

Затем соберите ответы и запишите их на доске.

Подведите итог сессии. Выделите некоторые ключевые моменты:

- Ключевые стратегии - "почему" и "как" - которые возникли в ходе обсуждения.

- Полученная в ходе занятия ключевая информация о ситуации, необходимая для того, чтобы лучше оценить ее.
- Свяжите это занятие с оценкой риска в том смысле, что в этом упражнении участники_цы рассмотрели ситуацию (темная улица) и приняли в этой связи решение в отношении своей безопасности и защите, основываясь на контексте, опыте и интуиции. И это было сделано быстро.
- Ощущение безопасности при движении по темной улице ночью - распространенный опыт. И как в этот момент мы можем оценить риски - насколько опасна эта улица? Как быстро я смогу бежать? Есть ли на этой улице места, где я могу попросить о помощи, на всякий случай? Иду ли я один_на? Есть ли на этой улице места, где кто-то может подстеречь меня? -- и применить стратегии и тактики для их снижения. Мы уменьшаем риски инстинктивно - как механизм выживания. Об этом важно помнить, когда вы приступаете к оценке рисков.
- Зная потенциальные риски в конкретной ситуации, каждый из нас может придумать стратегию и тактику, которые позволят снизить риски в сложившейся ситуации.

Примечания для фасилитатора_ки

- Очень важно, чтобы в первой части этого упражнения, в процессе рефлексии участников_ц по поводу способов самостоятельного безопасного передвижения по улице, они не переборщили с размышлениями. Именно поэтому достаточно пяти минут. Здесь мы хотим подчеркнуть важность инстинкта и жизненного опыта в оценке рисков в данной ситуации.
- Если вы почувствуете, что кто-то из участников_ц или все они напряжены из-за необходимости говорить об опыте передвижения по темной улице, сделайте перерыв. Дайте участникам_цам возможность отдышаться. Также предоставьте участникам_цам возможность отказаться от этого упражнения.
- Смысл этого занятия заключается в том, чтобы начать изучать оценку рисков. Здесь не важно соответствие данного задания стандарту: риск = угроза х вероятность х воздействие / потенциал. Важно, чтобы участники_цы смогли сформулировать причины, по которым они выбрали конкретную тактику передвижения по темной улице ночью.

- Повторите, что не существует правильных или неправильных ответов. Есть лишь ответы, основанные на опыте и рассуждениях.
- Если, основываясь на своих знаниях об участниках_цах, вы обнаружите, что выполнение связанного с передвижением по улице в одиночку ночью задания может вызвать обострение их прошлых травм, вы можете в качестве альтернативы выбрать для выполнения этого упражнения многолюдную улицу в дневное время, поскольку это может быть не столь травматично для участников_ц. Или многолюдную улицу ночью, где можно собрать различные виды элементов для осмысления риска. Ниже приведены примеры фотографий, которые вы можете использовать:

day_market.jpg
Image not found or type unknown

Фотография: Карл Кэмпбелл «Толпа на субботнем рынке Эль Чопо», фото с платформы Flickr.

night_market.jpg
Image not found or type unknown

Фотография: Вайчен Сю «Ночной рынок Шилинь», фото с платформы Flickr.

*Картинка с рисунком. На рисунке растения болотного цвета

image-1605451879726.png
Image not found or type unknown

Переосмысление риска и пять слоев риска [Углубленное Упражнение]

deepening_activ_circular_400px-with-text_russian.png
image not found or type unknown

Картинка. Надпись на картинке: Углубленные Упражнения
Рисунок на картинке: зеленый круг. Сверху картины дерево и по всему кругу распущены корни

На данный момент у нас есть только некоторые идеи о том, как переосмыслить риск. Это не было преобразовано в учебный модуль.

Переосмысление риска и оценка риска

Реалистичное понимание риска

Одной из проблем оценки риска в привычном понимании является обширность того, что подразумеваем, когда говорим "риск". Если рассматривать риск с точки зрения холистического подхода, то это еще больше расширяет значение этого понятия (что вполне оправданно). Цель оценки риска заключается в том, чтобы человек мог выработать стратегию и тактику для снижения рисков, с которыми он сталкивается, и мог принимать более обоснованные решения.

Часто ¨риск¨ рассматривают как все, что может пойти не так в ситуации, при этом не конкретизируя, на каких рисках можно сфокусироваться.

Другой способ более тонкой оценки риска заключается в том, чтобы рассматривать его с трех разных углов:

- Известные риски: Угрозы, которые уже были осуществлены в сообществе. Приведите примеры. Каковы причины? Каковы последствия?
- Возникающие риски: Угрозы, которые уже возникли, но не в рамках сообщества, к которому принадлежит человек. Это могут быть угрозы, возникающие в связи с текущим политическим климатом, технологическим развитием и/или изменениями в более широких активистских сообществах.
- Неосознаваемые риски: Это угрозы, которые невозможно предугадать, и нет способа узнать, возникнут ли они и когда.

Еще один способ начать думать о рисках - рассмотреть следующие слои:

FTX_Movement.png
Image not found or type unknown

Картинка, на картинке два круга, серый и красный. между серым и красным кругом надпись: "Инфраструктура / пространство". В красном кругу сверху в центре надпись: "Движение (контр движение)". В центре две фигуры зеленого и фиолетового цвета, под

каждой фигурой надпись: "Индивидуальное поведение/практика". Между фигурами стрелочка с надписью: "Межличностные/реляционные".

Слой инфраструктуры/пространства

Этот слой представляет собой пространство, в котором мы перемещаемся, общаемся и взаимодействуем. Это офлайн и онлайн пространства, где мы практикуем наш активизм. Где бы мы ни находились, существуют параметры, и эти параметры могут быть источниками рисков.

Например, один известный факт об Интернете заключается в том, что ничто в нем не может быть удалено навсегда. Какие риски это создает для активистов в интернете? Как этот факт может способствовать эскалации угроз?

Движение (контр движение)

Следующий уровень - это противостояние движений, к которым мы принадлежим, и тех, кто является нашими оппонентами. Каковы возможности наших движений? И каковы возможности наших оппонентов? Каким рискам мы подвергаемся по умолчанию, будучи частью феминистских движений? Кто наши союзники? Кто наши враги? И какие угрозы они представляют для нас?

Размышления о рисках в терминах движения также расширят наше понимание последствий реализованных угроз? Каковы последствия, помимо индивидуальных или организационных, гендерных притеснений в Интернете? Как это влияет на то, как наши движения могут использовать интернет для своей правозащитной деятельности?

Реляционный / межличностный слой

Одно из предположений, с которым многие активисты не сталкиваются, - недостаток доверия и недоверчивость, которые существуют внутри активистских сообществ. Да, важно строить доверительные отношения. Не менее важно определить уровень доверия, который существует между феминистскими активист(к)ами.

Индивидуальное поведение / практики

Как общается каждый из нас? Как мы выходим в интернет? Каковы предварительные реалии, в которых мы существуем в моменты взаимодействия? К какому оборудованию мы имеем доступ? Какие инструменты мы используем? Какими навыками мы обладаем? Индивидуальное поведение / практика отвечает на эти вопросы.

Для того чтобы глубже понять риск, важно исследовать эти слои.

Континуум поведения / практики и угрозы

В этой схеме мы начинаем с известной угрозы (или с тех, с которыми наши участники имели опыт) и изучаем поведение / практику, которые делают угрозу реальной и способствуют ее эскалации, а также дальнейшее поведение / практику, которые позволяют угрозе расти.

FTX_Continuum.png
Image not found or type unknown

Картинка: на картинке пять прямоугольников с текстом. Каждый прямоугольник связан стрелочкой. Левый, нижный угол: "Поведение / практика, которые приводят к эскалации: Один пароль для всех моих аккаунтов Не удалять личные сообщения в социальных сетях Хранение личных данных на моем аккаунте в социальных сетях". Стрелочки ведут к центру, надпись: "Эскалация угрозы: Частная информация обо мне становится известной другим" и к правому нижнему углу, надпись: "Частная информация о моей семье, друзьях и сетях становится известной другим людям". Верхний левый угол, надпись: "Практикуемое мною поведение, которое приводит к этой угрозе: Единый пароль для всех моих аккаунтов; Доступ к моим аккаунтам при небезопасном доступе в Интернет; Потеря оборудования. Стрелочки ведут к центру, надпись: "Угроза: Потеря доступа к моим аккаунтам в социальных сетях" и затем к двум эскалациям угроз, упомянутых выше.

Вторым уровнем для этой структуры будет определение стратегий снижения воздействия и реагирования в каждой точке изображения.

*Картинка с рисунком. На рисунке растения красного цвета

image_1605451259399.png

Image not found or type unknown

Упражнение: «Жизненный цикл данных как способ понимания риска» [Углубленное упражнение]

Данное обучающее упражнение направлено на рассмотрение оценки рисков с точки зрения жизненного цикла данных. Активисты_ки, организации и движения работают с данными - от создания / сбора / сбора данных до публикации информации, основанной на данных.

Введение

Image not found or type unknown deepening_activ_circular_400px-with-text_russian.png

Картинка. Надпись на картинке: Углубленные Упражнения

Рисунок на картинке: зеленый круг. Сверху картины дерево и по всему кругу распущены корни

Данное обучающее упражнение направлено на рассмотрение оценки рисков с точки зрения жизненного цикла данных. Активисты_ки, организации и движения работают с данными - от создания / сбора / сбора данных до публикации информации, основанной на данных.

Существует два основных подхода к технике проведения данного мероприятия:

- **Общий семинар** проводится в рамках общего семинара по цифровой безопасности, участники_цы которого представляют различные организации и/или не принадлежат к каким-либо организациям.
- **Организационный семинар** предназначен для отдельных групп и их сотрудников_ц. Общий контекст для этого типа семинара заключается в том, что различные команды одной организации объединяются для оценки рисков, связанных с практикой и процессами работы с данными в их организации.

Цели обучения и общие темы, рассматриваемые в обоих подходах, одинаковы, но методологии и техники фасилитации должны быть скорректированы для двух различных сценариев семинаров.

Цели обучения

В процессе выполнения этого упражнения участники_цы смогут:

- понимать риски и аспекты безопасности на каждом этапе жизненного цикла данных;
- применять механизмы оценки рисков для обеспечения личной и/или организационной безопасности.

Для кого предназначено данное упражнение?

Это упражнение предназначено для отдельных активистов_к (в рамках общей оценки рисков или семинара по цифровой безопасности) или для группы (организации, сети,

коллектива), проходящей процесс оценки рисков. Существуют две техники проведения, два подхода к этому упражнению, в зависимости от того, будет ли это общий семинар или занятие для отдельной группы.

Упражнение также может быть использовано в качестве диагностического для определения приоритетов, на каких практиках или инструментах следует сосредоточиться в оставшейся части семинара по цифровой безопасности.

Продолжительность

Зависит от количества участников_ц и размера группы. В целом, процесс может занять минимум четыре часа.

Ресурсы

- Бумага для флипчарта
- Маркеры
- Проектор для презентации жизненного цикла данных и направляющих вопросов, а также для совместного использования участниками_цами, если необходимо.

Техника проведения для общего семинара

(Этот материал предназначен для общего семинара по оценке рисков или цифровой безопасности, в котором участвуют активисты_ки из разных контекстов. Цели обучения остаются теми же, но некоторые тактики обучения и фасилитации будут отличаться от семинара для уже сформировавшейся группы людей.)

Первая фаза: что вы публикуете?

В этой части упражнения участникам_цам задается вопрос: «**Что вы публикуете в рамках своей работы в качестве активиста_ки?**»

Смысл здесь в том, чтобы начать с самой очевидной части жизненного цикла данных - обработанных данных, которые распространяются в виде информации. Это могут быть отчеты об исследованиях, статьи, сообщения в блогах, руководства, книги, веб-сайты, сообщения в социальных сетях и т. д.

Это можно сделать на пленарном обсуждении, в стиле "попкорн". Это когда ведущий_ая задает вопрос и просит участников_ц дать короткие и емкие ответы - как кукуруза, лопающаяся на сковороде!

Вторая фаза: презентация жизненного цикла данных и соображений по безопасности

Цель презентации - напомнить участникам_цам о цикле управления данными. Ключевые моменты презентации можно найти здесь (см.файлы основы-жизненного цикла данных-презентация.odp а также Презентация*)*.

Третья фаза: время рефлексии о жизненном цикле персональных данных

Сгруппируйте участников_ц в соответствии с тем, что они публикуют. Попросите их выбрать конкретный пример того, что они опубликовали (статья, исследовательский отчет, книга и т.д.), и попросите их сформировать группы на основе аналогичной работы.

Здесь у каждого_й из них будет время проследить жизненный цикл опубликованных данных, а затем у группы будет время поделиться своими рефлексиями.

Время на рефлексию должно составлять около 15 минут. Далее потребуется около 45 минут на обсуждение в группе.

Вопросы для индивидуальной рефлексии будут представлены в презентации.

При работе в группе все участники_цы группы по очереди расскажут о жизненном цикле данных своей опубликованной работы.

Четвертая фаза: обратная связь и соображения по безопасности

Вместо презентации групповых отчетов тренер_ка-фасилитатор_ка задает каждой группе вопросы, которые помогут выявить то, о чем шла речь в группах.

Ниже приведены вопросы, которые вы можете использовать для подведения итогов времени, проведенного в рефлексии и групповой дискуссии:

- Какие устройства хранения данных были наиболее распространены в группе? Какие из них использовал только один человек?
- Каковы были различия и сходства в доступе к хранилищу данных в вашей группе?
- Как насчет обработки данных? Какие инструменты использовались в вашей группе?
- Опубликовал ли кто-нибудь в группе что-то, что подвергло риску его или кого-то из его знакомых? Что именно?
- Задумывался ли кто-нибудь в группе о практике архивирования и удаления данных до сегодняшнего дня? Если да, то какова была практика в этой области?
- Возникали ли на каком-либо этапе жизненного цикла ваших данных проблемы с безопасностью и защитой? Каковы они?

Подведение итогов упражнения

По завершении групповых презентаций и обмена опытом тренер_ка-фасилитатор_ка может подвести итоги упражнения:

- Указать на ключевые моменты
- Спросить участников_ц об основных выводах, сделанных в ходе упражнения
- Спросить участников_ц об изменениях в практике управления данными, о которых они узнали в ходе мероприятия.

*Картинка с рисунком. На рисунке растения синего цвета

image-1605452256072.png

Техника проведения для организационного семинара

> Данный семинар предназначен для организаций и их сотрудников_ц.

Первая фаза: какая информация является общей для каждого отдела/ программы / команды организации?

Исходя из конфигурации и структуры организации, попросите каждый отдел или команду привести пример чего-то общего для них - внутри организации или за ее пределами.

- Вот примеры для стимулирования ответов:
- Для отделов коммуникаций - какие сводки вы публикуете?
- Для исследовательских команд - какие исследования вы проводите, о чем отчитываетесь?
- Для администраторов и финансистов - кто может ознакомиться с платежными ведомостями вашей организации? Как насчет финансовых отчетов?
- Для отделов кадров - как насчет оценки персонала?

> **Примечание по фасилитации:** на этот вопрос гораздо легче отвечать командам, у которых есть цели, ориентированные на внешний мир, например, отделу по коммуникациям, или программе, которая публикует отчеты и исследования. В отношении более ориентированных на внутренний мир отделов, таких как финансово-

административный или отдел кадров, тренеру_ке-фасилитатору_ке, возможно, придется потратить время на примеры того, какой информацией они обмениваются.

Цель этого этапа - заставить различные команды признать, что все они обмениваются информацией, как внутри организации, так и за ее пределами. Это важно, поскольку каждая команда должна быть в состоянии определить один или два вида информации, которыми они обмениваются при оценке риска в своей практике управления данными.

Вторая фаза: презентация жизненного цикла данных и соображений по безопасности

Цель презентации - напомнить участникам_цам о цикле управления данными. Ключевые моменты презентации можно найти здесь Презентация_Жизненный Цикл Данных

Третья фаза: групповая работа

В рамках команд попросите каждую группу определить один-два вида информации, которой они делятся/которую публикуют.

Чтобы расставить приоритеты, предложите командам подумать о том, какую информацию они больше всего хотят обезопасить, или о том, какая информация, которой они делятся, является конфиденциальной.

Затем, для каждого вида совместно используемой или публикуемой информации, попросите команды вернуться назад и отследить его жизненный цикл данных. Используйте приведенную ниже презентацию, чтобы задать ключевые вопросы о практике управления данными для каждого фрагмента опубликованных или совместно используемых данных.

В конце этого процесса каждая команда должна быть в состоянии поделиться с остальными результатами своих обсуждений.

В целом групповая работа займет около часа.

Четвертая фаза: презентации групп и рефлексия по поводу безопасности

В зависимости от размера организации и проделанной каждым отделом работы, дайте им время представить результаты обсуждения своим коллегам. Поощряйте каждую группу подумать о креативной презентации и ключевых моментах своих обсуждений. Им не обязательно делиться всем.

Призовите слушателей делать записи о том, что им рассказывают, поскольку после каждой презентации будет дано время для обмена комментариями и обратной связи.

В реалистичных условиях этот процесс займет около 10 минут на группу.

Роль тренера_ки-фасилитатора_ки здесь, помимо учета времени и управления обратной связью, заключается также в предоставлении обратной связи по каждой презентации. Сейчас самое время надеть шляпу практикующего специалиста по безопасности.

Некоторые области, о которых следует спросить:

- Если процесс сбора данных должен быть конфиденциальным, не лучше ли использовать более безопасные средства связи?
- Кто имеет доступ к устройству хранения данных в теории и в реальности? Если речь идет о физическом устройстве хранения данных, то где оно находится в офисе?
- Кто имеет доступ к исходным данным?

Как тренер_ка-фасилитатор_ка, вы также можете использовать эту возможность, чтобы поделиться некоторыми рекомендациями и предложениями по повышению безопасности практики управления данными в организации.

> **Примечание для фасилитатора_ки:** существует ресурс под названием Alternative Tools in Networking andCommunications («Альтернативные инструменты для нетворкинга и коммуникаций») в «FTX: перезагрузка безопасности», с которым вы можете ознакомиться для проведения данного упражнения.

Пятая фаза: возвращение к группам: улучшение безопасности

После того, как все команды представили свои презентации, они возвращаются в свои группы для дальнейшего обсуждения и рефлексии по поводу того, как они могут лучше защитить свой процесс управления данными и собственно данные.

Цель каждой группы - спланировать методы повышения безопасности на всех этапах жизненного цикла данных.

К концу обсуждения каждая группа должна иметь некоторые планы по повышению безопасности своей работы с данными.

> **Примечание:** предполагается, что для этого группа прошла базовый тренинг по безопасности. Как вариант, тренер_ка-фасилитатор_ка может использовать четвертую фазу как возможность предоставить некоторые рекомендации по более безопасным альтернативным инструментам, опциям и процессам для практики управления данными группы.

Методические вопросы для обсуждения в группе

- Какие из данных, которыми вы управляете, являются общедоступными (о них может знать каждый), частными (о них может знать только организация), конфиденциальными (о них может знать только команда и определенные группы внутри организации) - и как ваша команда может гарантировать, что эти различные типы данных могут оставаться частными и конфиденциальными?
- Как ваша команда может обеспечить контроль над тем, кто имеет доступ к вашим данным?
- Какова политика содержания и удаления данных на платформах, которые вы используете для хранения и обработки данных в интернете?
- Как команда может практиковать более безопасные коммуникации, особенно в отношении частных и конфиденциальных данных и информации?
- Какие практики и процессы должна иметь команда, чтобы сохранить конфиденциальность и секретность данных?
- Что следует изменить в вашей практике управления данными, чтобы сделать ее более безопасной? Посмотрите на результаты предыдущей групповой работы и определите, что можно улучшить.

- Какие роли должны быть у каждого члена команды, чтобы управлять этими изменениями?

Шестая фаза: финальная презентация планов

На этом этапе каждой команде будет предоставлено время для представления способов, которыми они будут обеспечивать безопасность своей практики управления данными.

Это возможность для всей организации поделиться стратегиями и тактиками и поучиться друг у друга.

Подведение итогов упражнения

После завершения групповых презентаций и обмена мнениями тренер_ка-фасилитатор_ка может подвести итог упражнения:

- Указать на ключевые моменты
- Спросить участников_ц об основных выводах, сделанных в ходе упражнения
- Согласовать дальнейшие шаги по практической реализации планов.

Презентация

Существует еще один способ понять риски по возрастанию — это взглянуть на практику работы с данными в организации. Каждая организация имеет дело с данными, и каждое отделение внутри организации тоже.

Ниже приведены некоторые аспекты безопасности и защиты для каждого этапа жизненного цикла данных.

Создание / получение / сбор данных

- Какого рода данные собираются?

- Кто создает/получает/собирает данные?
- Подвергнет ли это людей риску? Кто подвергнется риску в случае обнародования этих данных?
- Насколько публичным / частным / конфиденциальным является процесс сбора данных?
- Какие инструменты вы используете для обеспечения безопасности процесса сбора данных?

Хранение данных

- Где хранятся данные?
- Кто имеет доступ к хранилищу данных?
- Какие методы / процессы / инструменты вы используете для обеспечения безопасности устройства хранения данных?
- Облачное хранилище в противовес физическому хранилищу или хранилищу на устройстве.

Обработка данных

- Кто обрабатывает данные?
- Будет ли анализ данных подвергать риску отдельных лиц или группы лиц?
- Какие инструменты используются для анализа данных?
- Кто имеет доступ к процессу/системе анализа данных?
- При переработке данных сохраняются ли вторичные копии данных в других местах?

Публикация/обмен информацией из обработанных данных

- Где публикуется информация / знания?
- Будет ли публикация информации подвергать людей риску?
- Кто является целевой аудиторией публикуемой информации?
- Есть ли у вас контроль над тем, как публикуется информация?

Архивирование

- Где архивируются данные и обработанная информация?
- Архивируются ли исходные данные или только обработанная информация?
- Кто имеет доступ к архиву?
- Каковы условия доступа к архиву?

Удаление

- Когда происходит уничтожение данных?
- Условия удаления?
- Как мы можем убедиться, что все копии удалены?

Примечание для фасилитатора_ки

Это упражнение - хороший способ узнать и оценить контекст цифровой безопасности, практику и процессы участников_ц. Хорошо бы сосредоточиться на этом аспекте, а не ожидать от этого упражнения выработки стратегий и тактик для повышения их цифровой безопасности.

В рамках организационного семинара вы, возможно, захотите обратить внимание на кадровые и административные команды / отделы. Во-первых, во многих организациях, как правило, именно у этих сотрудников_ц не было опыта участия в семинарах по цифровой безопасности, поэтому многие темы и вопросы могут быть для них новыми. Во-вторых, поскольку большая часть их работы является внутренней, они могут не воспринимать свои подразделения как ¨публикующие¨ что-либо. Однако во многих организациях эти подразделения хранят и обрабатывают большое количество конфиденциальных данных (информация о персонале, зарплаты сотрудников, записи заседаний совета директоров, банковские реквизиты организации и т. д.) – поэтому важно указать на это в ходе семинара.

Обратите внимание и на физические устройства хранения данных. Если есть картотеки, где хранятся печатные копии документов, спросите, где они расположены, и кто имеет к ним физический доступ. Иногда существует тенденция слишком сильно концентрироваться на практике онлайн-хранилищ, упуская при этом возможность сделать более безопасной

тактику физического хранения.

Дополнительное чтение (по желанию)

- FTX: перезагрузка безопасности: альтернативные инструменты для нетворкинга и коммуникаций - FTX Safety Reboot: Alternative Tools in Networking and Communications.
- FTX: перезагрузка безопасности, модуль мобильной безопасности
- Electronic Frontier Foundation's Surveillance Self-Defense – Хотя это руководство в основном рассчитано на американскую аудиторию, в нем есть полезные разделы, объясняющие концепции наблюдения и инструменты, используемые для их обхода.
- Front Line Defenders' Guide to Secure Group Chat and Conferencing Tools – полезное руководство по различным безопасным чат- и конференц-сервисам и инструментам, которые соответствуют критериям Frontline Defender о том, что делает приложение или сервис безопасным.
- Mozilla Foundation's Privacy Not Included website – в котором рассматриваются различные политики и практики конфиденциальности и безопасности различных сервисов, платформ и устройств на предмет их соответствия Mozilla´s Minimum Security Standards (минимальным стандартам безопасности Mozilla), которые включают шифрование, обновления безопасности и политики конфиденциальности.

*Картинка с рисунком. На рисунке растения красного цвета

image-1605451259399.png

Организация протестов и оценка рисков [Тактическое Упражнение]

Это упражнение предназначено для того, чтобы помочь группе планирующих протест людей обдумать и устранить риски и угрозы, с которыми они могут столкнуться. Данное упражнение может быть применено для протестов, которые проводятся как в оффлайн, так и в онлайн, а также для протестов, которые имеют оффлайновые и онлайновые компоненты.

введение

tactical_activ_circular_400px-withtext_russian.png
Image not found or type unknown

Картинка. Надпись на картинке: Тактические Упражнения

Рисунок на картинке: оранжевый круг. В центре круга синее дерево с плодами

Это упражнение предназначено для того, чтобы помочь группе планирующих протест людей обдумать и устранить риски и угрозы, с которыми они могут столкнуться. Данное упражнение может быть применено для протестов, которые проводятся как в оффлайн, так и в онлайн, а также для протестов, которые имеют оффлайновые и онлайновые компоненты.

Данное упражнение не является занятием по планированию протеста, а скорее упражнением по оценке рисков протеста. Предполагается, что до проведения этого упражнения группа уже провела первоначальное планирование того, в чем будет состоять протест, а также его основных стратегий, тактик и действий.

Цели обучения

В ходе этого мероприятия участники_цы должны:

- осознать различные риски, с которыми они сталкиваются при проведении акций протеста
- создать план реагирования на выявленные риски для проведения более безопасного протеста?

Это упражнение полезно для группы людей (организаций, сетей, коллективов), которые договорились о совместном планировании протеста.

Группа должна провести предварительное планирование своего протеста, чтобы основные стратегии, тактики и действия были обсуждены и согласованы до начала этого упражнения.

Продолжительность

Это упражнение займет как минимум четыре часа.

Ресурсы

- Большая стена, к которой можно прикрепить бумагу для заметок и флипчарта. Если подходящей стены не окажется, расчистите пространство на полу, чтобы участники_цы могли выполнять эту работу вместе.

- Маркеры
- Клейкие стикеры
- Устройства, на которых можно вести электронное документирование обсуждений. При этом важно назначить людей в группе для документирования обсуждений и убедиться, что в случае обмена документацией она будет передаваться по защищенным каналам.

Техника проведения семинара по групповому планированию совместного протеста

Данное упражнение состоит из трех основных фаз:

- Первая фаза заключается в рассмотрении риска с точки зрения организаторов, сторонников и противников как источников угроз (прямых и косвенных угроз, а также противостояния вариантам, когда протест может провалиться). Первая фаза разбита на три различных упражнения, которые разработаны для того, чтобы группа пришла к общему пониманию возможных рисков, которым подвергается запланированный протест.
- Вторая фаза посвящена разработке стратегии устранения возможных уязвимостей и неудач протеста, а также определению роли организаторов в плане снижения рисков.
- Третья фаза фокусируется на обеспечении безопасных внутренних коммуникаций между участниками.

Первая фаза: оценка того, откуда могут исходить риски

Эта фаза имеет несколько уровней участия и взаимодействия для оценки того, откуда могут исходить риски для протестов. Чтобы сделать методику более понятной, различные уровни были обозначены как «упражнения».

Подготовьте бумагу для флипчарта для каждого из следующих пунктов:

Организаторы протеста: группы и отдельные лица, участвующие в планировании протеста. К ним относятся также союзники.

Сторонники: группы и лица, от которых вы ожидаете поддержки или участия в акциях протеста.

Противники протеста: группы и лица, на которых негативно повлияет этот протест, а также те, кто их поддерживает.

Мероприятия в рамках протеста: запланированные действия в рамках протеста и места проведения этих действий. Мероприятия могут быть как **онлайн,** так и **оффлайн**.

Упражнение 1: определяем «кто» и «что» протеста

Дайте участникам_цам время и место, чтобы заполнить каждый из этих листов бумаги для флипчарта стикерами со своими ответами. В качестве альтернативы они могут просто писать прямо на бумаге для флипчарта.

> **Примечание по фасилитации:** чтобы провести эту работу более организованно, особенно если в группе более семи человек, разбейте участников_ц на четыре группы. Каждая группа начнет работать на одном листе бумаги для флипчарта. Одна группа может начать с "Союзников протеста", другая - со "Сторонников протеста" и так далее. Дайте им время, чтобы заполнить своими ответами лист флипчарта, затем попросите их перейти к следующему, и так далее пока все группы не поработают с каждым из листов. Обычно это называется World Cafemethodology (методика “Мировое Кафе”.

Упражнение 2: распаковываем организаторов, сторонников и противников

После того, как все листы бумаги для флипчарты будут заполнены ответами, участники_цы разделятся на две группы:

- Группа 1 возьмет лист флипчарта с союзниками и сторонниками
- Группа 2 возьмет лист флипчарта с противниками

Лист бумаги для флипчарта с «**Мероприятиями»** останется в общей зоне для всех желающих.

У каждой группы будет свой собственный набор методических вопросов, которые помогут начать раскрывать, где же в сферах их внимания существуют риски.

Для «Организаторов и сторонников» направляющими вопросами являются:

- Кто из организаторов в настоящее время сталкивается с угрозами? Каковы эти угрозы? Как это может повлиять на протест?
- Есть ли внутренние конфликты среди организаторов? О чем нам следует знать? Какое потенциальное влияние это может оказать на процесс организации?
- Кто из сторонников, которых мы ожидаем, потенциально может получить сильный отпор?
- Каких угроз или ответных действий можно ожидать? Происходили ли ранее подобные акции протеста, получившие отпор? Как это было?
- Где может произойти ответный удар или нападение? Знаете ли вы, какие социальные сети особенно часто используются противниками? Какое воздействие может иметь ответная реакция в оффлайновых реалиях, во время или после?

Для «Противников» направляющими вопросами являются:

- Кто из списка противников будет наиболее активно выступать против протеста?
- Где они собираются? Где они концентрируются в оффлайне и в онлайне?
- Кто является лидерами или влиятельными лицами среди противников?

- Каким возможностями они обладают?
- Что они могут предпринять против протеста и его участников?
- Как противники могут повлиять на планирование протеста?
- Как они могут сорвать запланированные мероприятия во время протеста?

Как может выглядеть ответный удар после протеста? Как противники могут попытаться лишить протест смысла посредством ответной реакции? На кого она будет направлена? Где это может происходить, и какова роль социальных сетей в этом процессе?

> **Примечание по фасилитации:** большинство протестов в наши дни имеют как онлайн, так и оффлайн компоненты. Приведенные выше вопросы применимы как к онлайн, так и к оффлайн сценариям, протестам и контекстам. Но если вы заметили, что участники_цы слишком много внимания уделяют оффлайн-контексту, то, возможно, подбросьте им вопросы об онлайн-контексте , в котором находятся организаторы, сторонники и противники. Если они склонны концентрироваться на онлайн-факторах, то подскажите им вопросы об оффлайн-контекстах. Спросите, как онлайн-деятельность или события могут повлиять на оффлайн, и наоборот.

Дискуссия в группе должна занять от 45 минут до 1 часа.

В конце групповой дискуссии каждая группа поделится результатами обсуждения. В ходе обсуждения каждая группа должна сфокусироваться на следующих вопросах:

Для группы «Организаторов/сторонников»:

- Кто из организаторов/сторонников в настоящее время сталкивается с угрозами? С какими угрозами они сталкиваются?
- С какой ответной реакциией, как вы ожидаете, столкнутся союзники и сторонники после участия в протесте?
- Существуют ли внутренние конфликты или противоречия, которые могут представлять опасность для протеста, и в чем они могут заключаться?

Для «Противников»:

- Кто из противников потенциально предпримет действия для срыва протеста?
- Какого рода нарушений вы ожидаете от них?

- Как это будет выглядеть на разных этапах протеста: при планировании, во время и после?

Хорошо также попросить группы быть настолько конкретными в своих ответах, насколько это возможно.

Упражнение 3: рефлексия по поводу возможной неудачи

Цель этого упражнения - выявить некоторые возможные варианты, когда протест может потерпеть неудачу.

После этого всем участникам_цам будет дано время на рефлексию над следующим вопросом: «**Чего вы НЕ хотите, чтобы произошло в этом протесте?»**

Для дальнейшего раскрытия этого большого вопроса вы можете спросить группу о следующем:

- Подумайте о ваших организаторах и сторонниках - какой возможный негативный эффект может оказать на них этот протест?
- Если протест проходит в оффлайне и онлайне, то как ваши противники могут сорвать протест в обоих пространствах?
- Подумайте о местах проведения ваших протестных мероприятий - что вы НЕ хотите, чтобы с ними произошло?
- Подумайте о ваших протестных мероприятиях - что может привести к их провалу?

Попросите участников_ц поразмышлять о дискуссиях, которые они провели, и об ответах, которые они услышали. Попросите их взять несколько минут на размышления, а затем записать свои ответы на отдельных клейких стикерах и приклеить их на стену.

Сгруппируйте ответы, чтобы выработать общие темы для дальнейшего обсуждения.

*Картинка с рисунком. На рисунке растения красного цвета

image-1605451259399.png

Вторая фаза: планирование стратегии и тактики снижения рисков

Упражнение 1: работа в группах по устранению возможных уязвимостей и провалов

На основе кластеров, выработанных в ходе выполнения третьего упражнения первой фазы, разделите участников_ц на группы.

Каждая группа обсудит следующие вопросы:

- Что вы можете сделать, чтобы предотвратить этот негативный исход?
- Какие стратегии, подходы, протоколы безопасности потребуются для предотвращения этого?
- Существуют ли различные стратегии для стадий планирования, во время протеста и после него?
- Что вы будете делать, если этот негативный исход станет реальностью? Какие шаги вы предпримете?
- Кто должен руководить этими стратегиями?

К концу обсуждения каждая группа должна иметь список подходов и стратегий, а также протоколов (правил) безопасности в отношении негативного исхода. Их следует записать на

бумаге для флипчарта и/или задокументировать в электронном виде. Организуйте их в соответствии с различными этапами протеста: до, во время и после. Каждая группа представит свои списки остальным группам для обсуждения.

Роль тренера_ки-фасилитатора_ки здесь заключается в том, чтобы обеспечить обратную связь по подходам и стратегиям, предложить улучшения (если необходимо) и найти общие стратегии среди групп.

Упражнение 2: дискуссия о ролях

В большой группе обсудите роли, необходимые для снижения негативных последствий, соблюдения протоколов безопасности, управления безопасными коммуникациями до, во время и после протестных событий. Важно, чтобы группа окончательно определила эти роли и тех, кто будет их выполнять.

Третья фаза: безопасная коммуникация

Здесь тренер_ка-фасилитатор_ка может ознакомить группу с вариантами безопасной связи во время проведения акции протеста.

После этого группа может потратить время на установку и проверку того, что общаться друг с другом по выбранному каналу вполне возможно.

Для планирования этой работы прочитайте раздел Alternative Tools for Networking and Communications (Альтернативные инструменты для нетворкинга и еоммуникаций) и Модуль по мобильной безопасности.

> **Примечание по безопасности:** один из способов использования этих инструментов - убедиться, что люди, которые ведут документирование, могут обмениваться копиями своих записей и документации по защищенным каналам связи.

Корректировки для общего семинара

В целом, упражнения по оценке рисков более эффективны, когда они проводятся с группами, имеющими общие цели, контекст и сценарии рисков (например, интервенции по оценке организационных рисков или оценка рисков для сети организаций). Поэтому данное упражнение было разработано для группы, которая уже планирует совместную акцию протеста и имеет некоторые первоначальные планы относительно совместного протеста. Но его можно скорректировать для более общего сценария цифровой безопасности для отдельных людей из разных контекстов, которые думают об организации собственного протеста со своими группами.

Чтобы адаптировать это упражнение для более широкого использования, проведение пробного протеста будет хорошим методом для того, чтобы участники_цы попрактиковались и получили уроки, которые они затем передадут в свои группы /сети / коллективы, которые, в свою очередь, смогут оценить риск своих реальных протестов.

Некоторые рекомендации по созданию модели протеста:

- **Поместите протест в реальность.** Важно поместить протест в реальный контекст, потому что тогда модель протеста будет иметь границы и параметры реального протеста, у участников_ц будет возможность быть более конкретными в своем анализе и стратегиях.
- Если все участники_цы из одной страны, то расположите протест в этой стране. Если они из разных стран, то проведите региональный протест.
- **Разработайте модель протеста по проблеме, которая находит отклик у участников_ц.** Таким образом, протест будет близок участникам_цам несмотря на то, что он вымышленный. Они наверняка организовывали и/или участвовали в подобном протесте в прошлом.
- **Изложите требования или цели протеста.** Сделайте их четко связанными с рассматриваемой проблемой, что поможет в выполнении упражнения.
- **Разработайте оффлайн- и онлайн-активности протеста.** Убедитесь, что при определении активностей протеста у вас наличествует сочетание онлайн и

оффлайн тактик. Будьте конкретны в отношении этих действий - где они будут происходить, когда они будут происходить, как долго они будут продолжаться?
- **Возьмите за основу реальный протест.** Если вы знаете о протесте, который может подойти для участников_ц вашего семинара, используйте его в качестве модели протеста.

Главное при создании модели протеста - постараться как можно больше имитировать реальный сценарий протеста. Опять же, наиболее эффективными при оценке рисков являются конкретные действия.

Вам также нужно будет найти способы и скорректировать время, чтобы участники_цы могли изучить и усвоить модель протеста. Вы можете поделиться подробностями модели протеста до тренинга, но не думайте, что все успеют прочесть его до семинара. Вы можете представить модель протеста в начале семинара и выдать раздаточные материалы, чтобы каждая группа имела под рукой информацию по мере прохождения этапов и упражнений данного занятия.

*Картинка с рисунком. На рисунке растения красного цвета

image_1605451259399.png

Image not found or type unknown

Основы оценки рисков [Базисный материал]

Введение

Мы постоянно оцениваем наши риски. Так мы выживаем. Это процесс, который не является уникальным для цифровой и/или информационной безопасности.

Когда мы прогуливаемся ночью по безлюдной улице и, исходя из нашего понимания ситуации, принимаем решения по какой стороне улицы идти, как себя вести, к чему быть готовой, как ходить: *Значится ли эта улица как опасная? Опасен ли район, в котором находится эта улица? Знаю ли я кого-нибудь на этой улице, кто мог бы прийти мне на помощь? Смогу ли я быстро убежать, если что-то случится? Есть ли у меня при себе что-нибудь ценное, чем я смогу откупиться? Есть ли у меня при себе что-нибудь, что может нанести мне больший вред? По какой части этой улицы я могу идти, чтобы избежать возможного вреда?*

Когда наши организации планируют новые проекты, мы рассматриваем возможные варианты их провала. Мы принимаем конструктивные решения, основываясь на том, что мы знаем о контексте и факторах, которые могут привести к тому, что проект не достигнет своих целей.

При организации протестов мы рассматриваем способы обеспечения безопасности протеста и тех, кто в нем участвует. Мы организуем системы партнерской поддержки. Мы обеспечиваем немедленную юридическую поддержку в случае ареста. Мы инструктируем участников_ц акции о том, как вести себя, чтобы избежать преследования со стороны властей. Мы разрабатываем стратегию мирного проведения протеста, чтобы снизить риск для участников_ц. В протесте участвуют люди, в чьи обязанности входит обеспечение его безопасности.

Оценка собственных рисков может быть практикой, которую мы проводим инстинктивно, оценка рисков является определенным процессом, который мы проходим - обычно коллективно - для того, чтобы знать, как нам избежать угроз и/или ответить на них.

Оценка рисков: онлайн и оффлайн

Оценка наших рисков в интернете по разным причинам не столь инстинктивна. Многие из нас не понимают, как работает интернет в чем состоят его угрозы и риски – а они продолжают развиваться и расти. Некоторые люди относятся к онлайн-деятельности, действиям и поведению в сети как к чему-то не ¨реальному¨, что имеет менее серьезные последствия, чем происходящее с нами физически. С другой стороны, те, кому знакомы ситуации, или кто сталкивались со случаями, в которых из-за действий в интернете пострадала «реальная» жизнь человека (люди, которых обманывали на сайтах знакомств, люди, чьи запретные связи в интернете стали достоянием общественности, или активисты, арестованные за высказывания против своего правительства), склонны к параноидальному отношению к интернету.

В действительности для многих активистов_к бинарность "онлайн/оффлайн" является ложной. Использование цифровых устройств (мобильных телефонов, ноутбуков, планшетов, компьютеров и т.д.) и интернет-сервисов, приложений и платформ (Google, Facebook, Viber, Instagram, WhatsApp и т.д.) является обычным делом в работе многих активистов_к - в организационной и адвокационной деятельности. То, как мы организуем и выполняем свою активистскую работу, менялось и будет продолжать меняться по мере развития и совершенствования технологий. Интернет и цифровые технологии являются важнейшей частью нашей организационной инфраструктуры. Мы используем их для общения, организации акций, формирования нашего сообщества, а также как площадку для нашей деятельности. Оффлайн- собрания и мероприятия по адвокации часто сопровождаются онлайн-взаимодействием, особенно в социальных сетях и с использованием хэштегов. В возникших в последнее время протестных движениях грань между онлайн- и оффлайн-мобилизацией, организацией и собраниями часто незрима.

Вместо того чтобы воспринимать происходящее в интернете как нечто отдельное от нашей физической реальности, думайте об оффлайн- <-> онлайн-реальностях как взаимосвязанных и взаимопроникающих. Мы существуем в этих реальностях одновременно большую часть времени. То, что происходит в одной, влияет на то, как мы существуем в

другой.

Это также означает, что риски и угрозы переходят из онлайн в оффлайн и наоборот. Например, передовые государственные стратегии слежки за активистами_ками и их движениями эксплуатируют небезопасное использование технологий (например, переход по непроверенным ссылкам, или скачивание и открытие непроверенных файлов) для того, чтобы иметь возможность собрать больше информации об активистах_ках, их группах и движениях, что в конечном итоге может привести к физическому наблюдению. Все, кто сталкивались с гендерно-обусловленным насилием онлайн (ГОНО), знают о психосоциальных последствиях таких нападений и преследований. Были также случаи, когда ГОНО перерастало в угрозу физической безопасности для тех, кто стали объектом нападок. Различные формы ГОНО (преследование, публикация личных данных, домогательства) являлись тактикой, используемой против феминисток и квир-активисток, чтобы угрозами заставить их замолчать и отступиться.

Размышления о взаимопроникающей природе угроз и рисков в онлайн- <-> оффлайн-режимах могут оказаться весьма сложными - *с чего начать оценку и понимание того, каковы эти угрозы, откуда они исходят, а также выработку стратегии действий в связи с ними?*

Что такое оценка риска?

Оценка риска — это *начало процесса* повышения сопротивляемости при реагировании на изменяющиеся контексты и угрозы. Цель оценки риска заключается в том, чтобы иметь возможность разработать стратегию и тактику для снижения рисков и принимать более обоснованные решения.

В общих чертах, риск — это вероятность причинения вреда, травм или потерь.

При оценке риска речь идет о способности (или отсутствии таковой) индивида / организации / коллектива реагировать на воздействие (воздействия) реализованной угрозы, или о способности индивида / организации / коллектива избежать реализации угрозы.

Существует известная формула для оценки риска:

Риск = угроза x вероятность x воздействие / потенциал

Где:

- Угроза — это любое негативное действие, направленное на человека / группу людей .
  - Прямые угрозы — это объявленное намерение причинить вред.
  - Косвенные угрозы — это угрозы, которые возникают в результате изменения ситуации.
  - При определении угроз важно определить, откуда исходит угроза. Еще лучше - от кого она исходит.
- Вероятность — это возможность того, что угроза станет реальной.
  - С вероятностью связана концепция уязвимости. Речь может идти о местоположении, практике и поведении индивида / группы, которые увеличивают возможности для реализации угрозы.
  - Речь также идет о возможностях групп / отдельных лиц, которые создают угрозу, особенно по отношению к человеку / группе, которым угрожают.
  - Чтобы оценить вероятность, спросите себя, есть ли у вас реальные примеры угроз человеку или группе людей, с которыми вы знакомы, и сравните эту ситуацию с вашей.
- Воздействие — это то, что произойдет при реализации угрозы. Последствия угрозы.
  - Воздействие может быть оказано на человека, организацию, сеть или движение.
  - Чем выше и больше количество последствий одной угрозы, тем выше риск
- Потенциал — это навыки, сильные стороны и ресурсы, к которым группа имеет доступ, для того, чтобы либо свести к минимуму вероятность угрозы, либо ответить на ее воздействие.

*Картинка с рисунком. На рисунке растения красного цвета

image-1605451259399.png

Image not found or type unknown

Пример из практики: угрозы & их нейтрализация

Пример из практики: Дейя

Для иллюстрации приведем вымышленный, но довольно распространенный опыт Дейи. Дейя - феминистка-активистка, которая использует свой аккаунт в Twitter для обличения тех, кто пропагандирует культуру изнасилования. В результате этого Дейя подвергается преследованию и угрозам в Интернете.

Больше всего ее тревожат угрозы, когда ей обещают узнать о ее месте жительства и поделиться этой информацией в интернете, для того чтобы предложить остальным нанести ей физический вред. В данном случае цель ясна - причинение физического вреда Дейе. Есть и другие угрозы, такие как давление на ее работодателей с целью уволить ее с работы, а также онлайн-преследование людей, о которых известно что они являются ее друзьями.

Для оценки рисков Дейя должна будет проанализировать эти угрозы и оценить их вероятность и влияние - чтобы спланировать, как можно снизить риски.

Угроза 1: узнать, где она живет, и поделиться этой информацией в интернете

Основная масса угроз поступает с аккаунтов в интернете, с большинством из которых она не знакома и не может проверить, являются ли они реальными людьми или поддельными аккаунтами. Некоторых из посылающих угрозы онлайн она знает как известных деятелей, которые часто принимают участие в нападках на женщин в интернете. Основываясь на том, каковы были их предыдущие действия, она знает, что личные данные иногда публиковались в интернете, и это вызывает реальное чувство страха за личную безопасность.

Есть ли у нее возможность избежать этого? Насколько вероятно, что ее преследователи и агрессоры узнают, где она живет? Ей необходимо выяснить, какова вероятность того, что ее

адрес либо уже есть в интернете, либо может быть опубликован одним из нападавших.

Для того чтобы оценить это, Дейя может начать с поиска информации о себе и информации, которая доступна о ней в интернете - посмотреть, есть ли физические пространства, которые связаны с ней, и укажут ли они на ее реальное физическое местоположение. Если она обнаружит, что ее домашний адрес доступен в интернете, может ли она что-то с этим сделать? Если она обнаружит, что ее адрес в настоящее время можно найти в интернете, что она может сделать, чтобы избежать публичного доступа к нему?

Дейя также может оценить, насколько уязвим и/или безопасен ее дом. Живет ли она в здании с охраной и протоколами доступа для тех, кто там не проживает? Живет ли она в квартире, которую ей придется обезопасить самостоятельно? Живет ли она одна? Каковы уязвимые места ее дома?

Дейя также должна будет оценить свои собственные возможности и ресурсы самозащиты. Если ее домашний адрес будет опубликован в интернете, сможет ли она сменить место жительства? Кто может оказать ей поддержку в это время? Есть ли органы власти, к которым она может обратиться за защитой?

Угроза 2: оказывать давление на работодателей Дейи, чтобы добиться ее увольнения

Дея работает в НПО, которая занимается правами человека, поэтому угрозы увольнения ее с работы нет. Но адрес офиса организации общеизвестен в городе и доступен на веб-сайте.

Угроза увольнения с работы для Дейи невелика. Но общедоступная информация о ее НПО может стать уязвимым местом для физической безопасности Дейи и ее сотрудников.

В этом сценарии организация должна провести собственную оценку рисков в ответ на угрозы, которым подвергается одна из ее сотрудниц.

Что делать с рисками? Общая тактика снижения рисков

Помимо выявления и анализа угроз, вероятности, воздействия и возможностей, оценка рисков также связана с составлением плана по снижению всех выявленных и проанализированных рисков.

Существует пять основных способов снижения рисков:

Признать риск и составить планы на случай непредвиденных обстоятельств

Некоторые риски неизбежны. Или некоторые цели стоят риска. Это не значит, что их можно отбросить. Планирование на случай непредвиденных обстоятельств — это представить себе риски и наихудшие последствия и принять меры по их устранению.

Избежать риска

Это означает снижение вероятности возникновения угрозы. Это может означать внедрение политик безопасности для обеспечения большей безопасности группы. Это также может означать изменения в поведении, которые повысят шансы избежать конкретного риска.

Контролировать риск

Иногда группа может решить сосредоточиться на последствиях угрозы, а не на самой угрозе. Контролировать риск означает снизить серьезность последствий.

Перенаправление риска

Привлеките сторонний ресурс для того, чтобы взять на себя риск и его последствия.

Мониторинг риска на наличие изменений в вероятности и последствиях

Обычно это тактика снижения незначительных рисков.

Пример из практики: Дейя

Используем пример Дейи снова: у нее есть варианты того, как поступить с рисками, с которыми она сталкивается, основанные на анализе каждой угрозы, вероятности возникновения каждой угрозы, последствий каждой угрозы и ее собственных возможностей

справиться с угрозой и/или последствиями угрозы.

В сценарии, когда домашний адрес Дейи уже можно найти в интернете, риск придется признать, и Дейя может сосредоточиться на разработке планов на случай непредвиденных обстоятельств. Эти планы могут варьироваться от повышения безопасности ее жилья до переезда. Что именно станет возможным, будет зависеть от существующих реалий и контекста, в котором находится Дейя.

Другой вариант для Дейи в этом сценарии заключается в том, чтобы попросить те источники, где ее адрес находится в открытом доступе, удалить контент. Но это ненадежная тактика. Она позволит избежать риска, если никто из преследователей не видел адреса. Но если кто-то заметил и сделал снимок экрана с этой информацией, то Дейя мало что сможет сделать, чтобы остановить распространение данных.

В сценарии, когда адрес Дейи не является общеизвестным и доступным в интернете, будет больше возможностей избежать риска. Что может сделать Дейя, чтобы ее домашний адрес не был обнаружен преследователями? В данном случае она может удалять посты с географическими метками, которые находятся рядом с ее домом, и перестать публиковать посты с географическими метками в реальном времени.

В обоих сценариях (является ли ее адрес публичным или нет) Дейя может предпринять шаги по снижению риска, сосредоточившись на защите своего жилья.

Хорошие стратегии снижения риска включают в себя размышления о превентивных стратегиях и реагировании на инциденты - оценку того, что можно сделать, чтобы избежать угрозы, и что можно сделать, если угроза реализована.

Превентивные стратегии

- Какие возможности у вас уже есть для предотвращения этой угрозы?
- Какие действия вы предпримете, чтобы избежать реализации этой угрозы? Как вы измените процессы в сети, чтобы предотвратить возникновение этой угрозы?
- Нужно ли для этого создавать какие-либо политики и процедуры?
- Какие навыки вам понадобятся для предотвращения этой угрозы?

Реагирование на инцидент

- Что вы будете делать, когда эта угроза будет реализована? Какие шаги вы предпримете, когда эта угроза возникнет?
- Как вы сможете свести к минимуму серьезность последствий этой угрозы?
- Какие навыки вам необходимы для того, чтобы принять необходимые меры в ответ на эту угрозу?

image-1605451259399.png

Напоминания

Оценка рисков привязана ко времени

Ее следует проводить в течение определенного периода времени - обычно, когда появляется новая угроза (смена правительства, изменение законов, изменения в политике безопасности платформы, например), становится известно об угрозе (преследование активистов_к в интернете, сообщения о взломе аккаунтов активистов_к), или происходят изменения в коллективе (новый проект, новое руководство, например). Следовательно, важно, чтобы оценка риска пересматривалась, поскольку риск меняется по мере появления и исчезновения угроз, а также по мере изменения способности группы и отдельных людей в этой группе реагировать и восстанавливаться после столкновения с угрозой.

Оценка риска не является точной наукой

Каждый человек, входящий в группу, которая оценивает риски, имеет свою точку зрения и позицию, что влияет на его способность осознавать вероятность реализации угрозы и свои собственные возможности избежать угрозы либо ответить на ее воздействие. Смысл оценки риска заключается в том, чтобы коллективно принять эти различные точки зрения в группе и составить общее понимание тех рисков, с которыми они сталкиваются. Оценка риска относительна. Разные группы людей могут сталкиваться с одинаковыми рисками и угрозами, но их способность избежать этих угроз и/или их способность реагировать на последствия угроз различны.

Оценка риска не обеспечит 100% безопасности, но она может подготовить группу к угрозам

Поскольку не существует такого понятия, как стопроцентная безопасность, оценка рисков не может гарантировать этого. Что она может сделать, так это дать возможность человеку или группе оценить угрозы и риски, которые могут потенциально повлиять на них.

Оценка рисков — это способность анализировать существующие и возникающие риски, чтобы выяснить, какие риски невозможно предсказать

Существуют разные типы рисков:

- Известные риски: угрозы, которые уже были осуществлены в отношении сообщества. Приведите примеры. Каковы причины? Каковы последствия?
- Возникающие риски: угрозы, которые уже возникли, но не в рамках сообщества, к которому принадлежит человек. Это могут быть угрозы, возникающие в связи с текущим политическим климатом, технологическим развитием и/или изменениями в более широких активистских сообществах.
- Непредвиденные риски: угрозы, которые невозможно предугадать, и нет возможности узнать, возникнут ли они и когда.

Оценка рисков важна при планировании

Она позволяет отдельным лицам или группам рассмотреть, что может причинить им вред, последствия этого вреда и их шансы на смягчение вреда и его последствий. Прохождение процесса оценки рисков позволяет группам принимать реалистичные решения о рисках, с которыми они сталкиваются. Это позволяет им подготовиться к угрозам.

Оценка риска — это способ справиться с тревогой и страхом

Это хороший процесс, который необходимо пройти, чтобы понять, чего боятся люди в группе - создать баланс между паранойей и полным отсутствием страха (паранойи), чтобы, действуя как группа, они могли принимать решения о том, к каким рискам следует

готовиться.

*Картинка с рисунком. На рисунке растения красного цвета

image-1605451259399.png

Оценка рисков при формировании движения [Базисный материал]

Обзор

Если рассматривать оценку рисков на уровне формирования движений, то это означает расширение сферы охвата и включение общих пространств, процессов, ресурсов или деятельности, которые управляются коллективно - формально или неформально.

Движения масштабнее, чем организации, и состоят из взаимоотношений совместной политической приверженности и действий между различными участниками_цами. Действующими лицами движения могут являться отдельные люди, организации, коллективы, члены сообществ или групп, которые привносят в движение различные знания, навыки, контексты и приоритеты. То, как участники_цы движения самоорганизуются, определяют роли и сферы ответственности и приходят к соглашениям, является важным аспектом в процессе формирования движения, где оценка рисков также может сыграть свою роль в выявлении потенциальных источников стресса.

Оценка риска с перспективы движения

Зачастую движения легче идентифицировать ретроспективно, поскольку они органично развиваются во времени и реагируют на проблемы конкретных контекстов и моментов. Порой мы думаем о движениях как о протестах, поскольку именно на этом этапе многие

движения становятся заметными и развиваются. Но не все движения заканчиваются (или начинаются) протестом. Например, многие движения ЛГБТКИ++ в местах, где открытость является дорогим удовольствием, организуют и предпринимают действия менее заметными способами, такими как создание закрытых сообществ в интернете, где люди могут собираться, общаться, оказывать поддержку и разрабатывать стратегии для различных видов интервенций.

Движение состоит из множества различных моментов или этапов, таких как работа с сообществом, сбор доказательств, углубление понимания, формирование консенсуса, принятие мер, создание пространства для коллективной заботы, распределение ресурсов и так далее.

Каждый из этих моментов или этапов может быть тем самым временем, когда коллективная оценка риска может быть предпринята теми, кто владеет пространством или процессом. Возможно, полезно думать о безопасности движения как о наличии условий, в которых многие этапы или компоненты работы с движением могут осуществляться и процветать.

Уровни риска

Один из способов начать процесс оценки риска с перспективы движений - распаковать различные уровни, которые необходимо рассмотреть. Есть три компонента, которые взаимодействуют друг с другом.

1. Взаимоотношения и протоколы
2. Пространства и инфраструктура
3. Данные и информация

В приведенных ниже разделах описано, что представляет собой каждый уровень и некоторые входящие в них компоненты, включая вопросы для обсуждения, которые могут помочь распаковать, проанализировать и понять риски для разработки план.

*Картинка с рисунком. На рисунке растения красного цвета

image-1605451259399.png
Image not found or type unknown

1. Взаимоотношения и протоколы

В основе сильных движений лежат прочные отношения, которые строятся на основе доверия. Это особенно важно, поскольку движение — это не столько форма, сколько сила и стойкость взаимоотношений на разных уровнях.

Оценка риска может происходить на уровне отдельного человека, организации или неформальных групп. Если подходить к оценке с перспективы формирования движения, то это значит обратить внимание на взаимосвязи между этими уровнями.

Например, если человек испытывает сильный стресс из-за того, что работает от зарплаты до зарплаты, это может повлиять на его способность в полной мере принимать участие, что, в свою очередь, может сказаться на организационной работе в целом. Или, если организация подвергается нападкам со стороны правительства, ее связи с другими организациями или отдельными людьми в движении могут и их также сделать уязвимыми для подобных атак. Или, если между членами коллектива существуют конфликты, это может ослабить движение в целом в результате как внешней, так и внутренней напряженности.

Другими словами, риск с перспективы движения — это то, что принимается коллективно, и на него влияют практики и благополучие различных точек пересечений /действующих лиц, которые являются частью организации движения.

Чтобы управлять рисками на уровне отношений, можно рассмотреть следующие три области :

а) Коллективная забота

Коллективная забота — это как индивидуальная, так и коллективная ответственность друг перед другом. Это означает, что при оценке и планировании рисков необходимо учитывать состояние самочувствия разных людей, а также их отношение друг к другу в плане общих пространств, платформ, ресурсов и процессов.

- Каковы некоторые из рисков в отношении благополучия, с которыми в настоящее время сталкиваются некоторые действующие лица группы?
- Какими могут быть некоторые последствия?
- Каков технологический слой данного вопроса, касающийся заботы и благополучия? Например, существуют ли протоколы по отстранению от социальных сетей, ограничения на онлайн-встречи или подключению активизма солидарности сторонних наблюдателей, когда на одного из членов группы нападают?
- Как можно разработать некоторые коллективные практики для смягчения или устранения некоторых рисков или видов воздействия? Есть ли ресурсы или навыки, которые можно объединить или использовать совместно? Например, могут ли различные организации или отдельные лица объединить ресурсы для подписки на более безопасный канал связи или хостинг, позволяющий лучше контролировать данные?

b) Инклюзивность и представленность

Это касается процессов и критериев включения людей в различные слои организационного пространства. Иногда об этом задумываются только когда уже произошло определенное нарушение безопасности, например, информация о мероприятии попала к недоброжелателям, потому что все происходит в одной группе Whatsapp или Facebook. Размышления о механизмах инклюзии могут помочь быть более целенаправленными в разработке различных уровней безопасности обмена информацией и каналов коммуникации. Соображения представленности в деятельности движения могут также помочь выявить особые риски для отдельных лиц или групп людей, а также способы смягчения и распределения этих рисков или подготовки к ним.

- Каковы протоколы, касающиеся привлечения новых людей или их ухода из группы/движения? Например, рассылка по электронной почте или другие виды дискуссионных и рабочих пространств.
- Существуют ли особые риски, связанные с участием одиночных лиц или многих людей в видимых моментах движения? Как это можно заранее спланировать? Например, когда публикуются призывы к участию, есть ли план, с каких аккаунтов они должны поступать (личные аккаунты, одноразовые аккаунты для конкретной деятельности, организационные аккаунты и т.д.), и в какие сроки, чтобы их нельзя было отследить до единого первоначального источника?

- Каковы некоторые риски, связанные с солидарными действиями с союзниками в конкретном случае, и как их можно предусмотреть? Например, получение согласия на сбор и размещение фотографий в социальных сетях, особенно от отдельных личностей, или распределение риска за счет большого количества людей.
- Каковы различные условия подключения к интернету и технические возможности участников_ц движения - и как это влияет на их способность безопасно участвовать в движении?

c) Управление конфликтами

- Этой области часто уделяется меньше всего внимания в движениях, поскольку мы предполагаем наличие общей политики, ценностей и интересов. Однако важно дать возможность выявить, обсудить и спланировать эти вопросы, поскольку они могут служить для поддержки общей миссии справедливости движения, а также обеспечить устранение внутренних уязвимостей или различий во власти.

  План не обязательно должен быть сложным, но он может начинаться с откровенного и подробного обсуждения, выявления общих ценностей и достижения договоренностей – с последующим составлением плана, включающим такие аспекты как кто должен быть вовлечен, какие меры могут быть приняты и как общие ценности могут быть коллективно реализованы.
- Каковы некоторые из потенциальных конфликтов, которые могут представлять опасность для движения? В частности, конфликты между членами движения? Каковы могут быть последствия? Например, потеря доверия, принятие членами сообщества чьей-либо стороны, потеря контроля над ресурсами движения, такими как пароли, доступ к сайтам и т. д.
- Как можно разработать план реагирования на различные виды конфликтов? Например, сексуальные домогательства внутри движения, насилие со стороны сексуального партнера между членами движения, романтические или сексуальные отношения между членами движения, которые закончились неудачно, принятие решений относительно общих ресурсов или финансирования, разногласия относительно основных ценностей или стратегий и т. д. Одни из них являются более долгосрочными, устойчивыми механизмами, в то время как другие могут зависеть от конкретной деятельности.

2. Пространства/инфраструктура

В наше время цифровой уровень становится все более важным компонентом для организации и создания движений. Поскольку движения не находятся в институциональном пространстве, цифровая инфраструктура и платформы становятся важным общим пространством для объединения, координации и планирования деятельности, документирования решений/прозрачности, а также живым архивом коллективной истории и т. д. Это критически важная часть экосистемы движений сегодня.

Часто цифровая инфраструктура движений представляет собой комбинацию различных платформ, инструментов и аккаунтов, которые внедряются или появляются со временем, развиваясь вместе с движением по мере его роста. В отличие от организации, в ней может быть несколько человек, заботящихся о разных видах пространств для разных целей, которые также могут служить разным сообществам. Некоторые из них могут быть действовать под личными аккаунтами, некоторые - под временными аккаунтами, созданными на время мероприятия или события, а некоторые могут оперировать подписками и пространствами, созданными специально для объединения различных потоков информации, контента и сообщества. Если уделить время пониманию этих пространств как экосистемы - взаимосвязанных компонентов общей инфраструктуры передвижения - и оценке потенциальных рисков, то это может помочь вывести на поверхность коллективную ответственность, заботу и управление этими пространствами, а также разработать планы безопасности в связи с возможными компромиссами.

Ниже перечислены области, которые можно обсудить при рассмотрении оценки риска для пространств и инфраструктуры, а также некоторые вопросы, которые можно рассмотреть:

a) Решения о платформе/инструменте/хостинге

Движение и организационная работа в значительной степени зависят от обмена информацией и эффективной коммуникации. Поэтому продумывание рисков, связанных с тем, какую платформу или инструмент использовать для организации, и где они будут храниться, может иметь большое влияние на безопасность людей, групп и работы движения. При оценке рисков, связанных с уязвимостью к нарушениям и атакам, может быть полезно рассмотреть, существуют ли разработанные феминистками/активистками или размещенные на хостинге решения для этой конкретной потребности, поскольку они обычно

уделяют больше внимания вопросам конфиденциальности и безопасности.

Также важно учитывать доступность, удобство использования, простоту и вероятность эффективного внедрения более крупными представителями движения. Не всегда полезно выбирать наиболее технически безопасное решение, если оно требует больших затрат времени и энергии, необходимых для того, чтобы научиться пользоваться им, что далеко не всегда возможно или целесообразно.

- Какие платформы, инструменты и пространства используются в настоящее время, для каких целей, и кто имеет к ним доступ?
- Каковы потенциальные риски, связанные с конкретными платформами/инструментами/хостингами, в отношении решения поставленной задачи? Каково влияние этих рисков?
- Какие знания, навыки и потенциал необходимы для освоения технологии? Как можно поделиться этими знаниями, навыками и возможностями с более широким кругом людей внутри движения, чтобы не создавать внутреннюю иерархию власти на основе технологий?
- Доступны ли эти технологии большинству людей, которым необходимо их использовать? Не приведут ли барьеры, препятствующие простоте использования, к созданию более небезопасных практик? Как это можно решить?
- Как распределить риски, одновременно распределив использование платформы/инструмента для конкретных целей?

b) Владение и обеспечение ресурсами

Владение и управление общей цифровой инфраструктурой — это и ответственность, и власть, и потенциальный контроль. Чем успешнее движение сможет превратить этот процесс в политический диалог об общих ценностях и понимании управления, экономики и построения сообщества, тем более устойчивыми будут некоторые из практик совместного использования технологий.

- Как будет обеспечиваться ресурсами использование конкретной инфраструктуры, платформы или инструмента? Как они обеспечиваются ресурсами в настоящее время? Какова внутренняя экономика совместного движения по распределению затрат, когда речь идет об использовании и приверженности конкретной технологии (технологиям)?

- Каковы риски использования "бесплатных" платформ, когда речь идет о контроле над данными и функциями, и риски платных услуг, когда речь идет о способности взять на себя обязательства по расходам на длительный период времени? Как их можно спрогнозировать?
- Как это может быть отражено в политиках движения? Например, разработка протоколов, касающихся общего владения, управления и обеспечения ресурсами. Можно ли заключить специальные, неформальные, легкие совместные экономические соглашения? Каким образом они могут быть устойчивыми и прозрачными?

c) Администрирование и протоколы

В контексте организации движения размышления об инфраструктуре как об общем пространстве означают, что ясность в отношении того, как и кем управляются эти пространства, может помочь не только проявить коллективную заботу, но и выявить потенциальные риски, связанные с доступом к информации и пространству сообщества, заботой о них и возможной их потерей.

- Кто имеет контроль над доступом к определенным пространствам? Насколько это зависит от того, кто владеет пространством (личные аккаунты) или настройками, и насколько это зависит от знаний, устройства или условий подключения для доступа?
- Каковы риски, связанные с компромиссами в отношении конкретных пространств? Откуда могут исходить эти риски (подумайте о внутренних и внешних угрозах), и каковы могут быть последствия? Как это можно спрогнозировать?
- Как осуществляется управление пространствами? Каковы протоколы, например, сколько человек имеют административный доступ, их местонахождение (отдельный человек, организация, сеть), как часто эти факторы меняются, условия изменения, смена паролей и т. д.?
- Существуют ли протоколы по удалению пространства или данных и архивированию? Или есть ли существующие практики, которые можно обсудить и перевести в протоколы?
- Как, где и когда проводятся обсуждения по оценке рисков для общей цифровой инфраструктуры?

- Кто будет реагировать в случае инцидентов в пространствах / инфраструктуре, которые влияют на безопасность движения?
- Какие изменения в пространстве, используемом движением (например, новые политики безопасности на платформах, или удаление функций безопасности, и т. д.) и в контексте движения (например, изменение ситуации в стране, смена правительства, новые законы, которые влияют на способность движения продолжать свою работу, и т.д.) вызовут более широкое обсуждение пространства / инфраструктуры в движении? Кто будет следить за этими изменениями?

*Картинка с рисунком. На рисунке растения красного цвета

image-1605451259399.png

3. Данные/информация

В процессе организационной деятельности постоянно производятся и генерируются данные и информация. Они могут быть представлены в форме формальных или неформальных, преднамеренных или теневых форм данных. Еще один способ оценить риски по возрастанию - рассмотреть практику данных в конкретной деятельности или стратегии движения. Подумайте об этом либо с точки зрения отдельной рабочей группы внутри движения, которая отвечает за выполнение конкретных задач или стратегий, либо с перспективы вида деятельности. Это также можно использовать на уровне организации, поскольку каждая организация имеет дело с данными, и каждое подразделение внутри организации тоже.

Здесь приведены некоторые соображения по безопасности и защите для каждой фазы жизненного цикла данных. В этом разделе есть упражнение "Жизненный цикл данных как способ понимания риска" (ССЫЛКА на упражнение), который оперирует этим разделом.

a) Создание/ получение/ сбор данных

- Какие данные собираются?
- Кто создает/получает/собирает данные?

- Подвергнет ли это людей риску? Кто подвергнется риску в результате обнародования этих данных?
- Насколько публичным / частным / конфиденциальным является процесс сбора данных?
- Какие инструменты вы используете для обеспечения безопасности процесса сбора данных?

b) Хранение данных

- Где хранятся данные?
- У кого есть доступ к хранилищу данных?
- Какие методы / процессы / инструменты вы используете для обеспечения безопасности устройства хранения данных?
- Облачное хранение в сравнении с физическим хранением и в сравнении с хранением на устройстве.

c) Обработка данных

- Кто обрабатывает данные?
- Будет ли анализ данных подвергать риску отдельных лиц или группы лиц?
- Какие инструменты используются для анализа данных?
- Кто имеет доступ к процессу/системе анализа данных?
- При обработке данных хранятся ли вторичные копии данных в другом месте?

d) Публикация/ обмен информацией из обработанных данных

- Где публикуется информация / знания?
- Подвергнет ли опубликованная информация людей риску?
- Кто является целевой аудиторией публикуемой информации?
- Есть ли у вас контроль над тем, как публикуется информация?

e) Архивирование

- Где архивируются данные и обработанная информация?
- Архивируются ли исходные данные или только обработанная информация?

- Кто имеет доступ к архиву?
- Каковы?

f) Удаление

- Когда происходит удаление данных?
- Каковы условия удаления?
- Как можно убедиться в том, что все копии удалены?

Заключение

Этот информационный документ призван помочь вам получить концептуальное представление о том, как рассматривать оценку рисков с перспективы формирования организаций движения. Часто оценка риска проводится на уровне отдельного человека или организации. Думать об этом на уровне движений означает попросить участников представить себя в качестве значимой, но парциальной части большего сообщества организаторов.

Когда общий контекст, цель или деятельность определены, это может помочь объединиться и продумать общий план в качестве общей почвы для групп людей, которые организованы по-разному. Это также может поспособствовать процессам коллективного размышления об устойчивости и организации путем предвидения и планирования в отношении рисков, связанных с групповой и реляционной динамикой, и там, где информационно-коммуникационные технологии играют важную роль в качестве инфраструктуры движения.

Вы можете поделиться этим в качестве дополнительного ресурса для подготовительного чтения с участниками_цами или выбрать конкретные уровни для дальнейшего углубления в качестве группового упражнения или обсуждения.

Дополнительная литература

в более широком смысле о понимании формирования движений и коллективных организаций, а также о цифровых реалиях:

- Информационно-коммуникационные технологии в создании феминистского движения: пособие для активисток: https://genderit.org/resources/icts-feminist-movement-building-activist-toolkit
- Создание феминистского интернета: формирование движения в цифровую эпоху: https://www.genderit.org/editorial/making-feminist-internet-movement-building-digital-age
- Достижение преобразующего феминистского лидерства: пособие для организаций и движений: http://awdflibrary.org/bitstream/handle/123456789/409/104951-283846-1-PB.pdf?sequence=1

*Картинка с рисунком. На рисунке растения красного цвета.

image-1605451259399.png