

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 х вероятность х 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

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

Revision #2
Created 24 April 2023 17:51:11 by Kira
Updated 26 April 2023 06:19:39 by Kira