ПОСОБИЕ ПО БЕЗОПАСНОСТИ
ДЛЯ
ПРАВОЗАЩИТНИКОВ

Разработано и составлено Энрике Эгуреном
«Пис Бригейдс Интернешнл», Европейский отдел (ПБИ/ЕО)

Опубликовано «Фронт Лайн»
Международным фондом защиты борцов за права человека

Издано «Фронт Лайн» -
Международным фондом защиты борцов за права человека, 2005
16 Idrone Lane, Off Bath Place, Blackrock, County Dublin, Ireland

Эту книгу можно заказать по таким адресам:
info@frontlinedefenders.org и pbibeo@biz.tiscali.be

Стоимость €20, исключая расходы на упаковку и доставку почтой

Все заказы и запросы относительно получения данного Пособия направляйте по таким адресам:

PBI-European Office
38, Rue Saint-Christophe, 1000 Bruxelles (Belgium)
тел./факс: + 32 (0)2 511 14 98
pbibeo@protectionline.org

Front Line
16 Idrone lane, Off Bath Place, Blackrock, County Dublin, Ireland
тел.: +353 1212 3750 факс: +353 1212 1001 эл.
почта: protectionmanual@frontlinedefenders.org

Настоящее Пособие переводится Фондом «Фронт Лайн» на французский, испанский, русский и арабский языки (а также на ряд других языков)

ISBN: 0-9547883-5-4

Предисловие – Хина Джилани

Работая специальным представителем Генерального секретаря ООН по делам правозащитников, я с всевозрастающей тревогой отмечаю рост числа сообщений о серьёзных нарушениях прав правозащитников и заметный сдвиг от умышленных действий низкого уровня, таких как запугивание и преследование, до более серьезных инцидентов - таких как угрозы физической неприкосновенности личности правозащитников и нападения на них. В 2004 году мы получили информацию о 47 правозащитниках, убитых за свою деятельность.

Понятно, что ответственность за безопасность правозащитников лежит в первую очередь на правительствах, как установлено Декларацией ООН о защитниках прав человека[1]. Нам следует продолжать работу, чтобы убедить правительства стран мира более серьезно придерживаться своих обязательств в этом направлении и принимать действенные меры для обеспечения безопасности правозащитников.

Опасность, связанная с повседневной деятельностью правозащитнико, тем не менее, такова, что очень важно совершенствовать и другие средства обеспечения их безопасности. В этой связи, я надеюсь, что данное Пособие по безопасности станет существенным подспорьем для правозащитников в разработке своих собственных систем и механизмов защиты. Многие правозащитники настолько погружены в работу по защите других, что порой уделяют слишком мало внимания своей собственной безопасности. Очень важно, чтобы все работающие в области отстаивания прав человека, осознавали важность соблюдения норм безопасности - не только своей сосбственной, но и тех, с кем и для кого они работают.

Хина Джилани, специальный представитель Генерального секретаря ООН по делам защитников прав человека

1 Декларация о праве отдельных лиц , общественных групп и организаций обеспечивать и уважать общепризнаные права и основные свободы человека и быть ответственными за это

Фонд «Фронт Лайн»

Фонд «Фронт Лайн» основан в Дублине в 2001 году специально для защиты правозащитников - людей, отстаивающих ненасильственными методами как отдельные, так и вместе взятые права, закрепленные во Всеобщей Декларации прав человека (ВДПЧ). «Фронт Лайн» стремится направлять свои силы на удовлетворение, прежде всего, тех нужд, на которые указывают сами правозащитники, включая защиту и безопасность, наведение контактов, обучение и обеспечение доступа к тематическим и региональным механизмам влияния ООН и других международных организаций.

Основной объект деятельности «Фронт Лайн» - это те правозащитники, которые временно или постоянно рискуют своей жизнью, действуя от имени и в интересах своих сограждан. Фонд «Фронт Лайн» осуществляет программу малых грантов, предусматривающих средства для обеспечения безопасности правозащитников. Фонд также организует кампании в защиту правозащитников, оказавшихся в условиях реальной угрозы для их жизни, и лоббирование от их имени. В чрезвычайных ситуациях, Фонд содействует их временному переселению в более безопасные регионы.

Фонд «Фронт Лайн» проводит исследования и публикует доклады о правозащитной ситуации в отдельных странах. Фонд также разрабатывает ресурсные материалы и учебные программы в помощь правозащитникам, а также способствует развитию связей и обменов между правозащитниками из различных стран мира. Проекты Фонда "Фронт Лайн" осуществляются, как правило, в сотрудничестве с рядом некоторых национальных правозащитных организаций.

"Фронт Лайн" содействует распространению осведомленности о положениях Всеобщей декларации прав человека и добивается того, чтобы принципы и нормы, определенные в "Декларации прав и ответственности отдельных лиц, общественных групп и органов поддерживать и защищать всеобщие права и основные свободы человека" (известную ещё как "Декларация о правозащитниках"), были известны, признаны и соблюдались во всём мире.

Фонд "Фронт Лайн" имеет специальный консультативный статус при Экономическом и социальном совете ООН.

Фонд "Фронт Лайн" имеет статус благотворительной организации (регистрационный номер CHY NO 14029) и является независимым и беспристрастным.

Для поддержки своей работы Фонд «Фронт Лайн» целиком полагается на великодушие отдельных лиц и благотворительность организаций. С самого начала своей деятельности в 2001 году, "Фронт Лайну" удавалось получать средства из множества источников. Фонд с благодарностью принимает дотации на индивидуальной основе.

Совет попечителей: Денис О'Брайен (председатель), Мэри Лолор (директор), Пьер Сане, Киеран Малви, Нолайн Блэкуэлл, Майкл Форст, Дэйвид Сайкс. Руководящий совет: Ханаан Ашрави, Робер Бадинтер, Боно, Его Святейшество Далай-Лама, Индаи Лурдес Сахор, Вангараи Мута Маатаи, Мартин О'Брайен, Адольфо Перес Эскивель, Десмонд Туту.

«Пис Бригейдс Интернешнл»

«Пис Бригейдс Интернешнл» (ПБИ) – это неправительственная организация (НПО), защищающая правозащитников и способствующая ненасильственной трансформации конфликтов.

Получив сигнал, ПБИ посылает группы добровольцев в зоны репрессий и конфликтов. В случае угрозы политического насилия, добровольцы берут правозащитников и их организации под свою опеку. Нарушители прав человека обычно стараются избегать обнародования их внеправовых действий. Физическое присутствие добровольцев в качестве наблюдателей, их деятельность по информированию правозащитного сообщества и отстаиванию его интересов, равно как и внушительная международная поддержка, которой они пользуются – всё это способствует сдерживанию враждебных действий и агрессии по отношению к правозащитникам. Таким образом, ПБИ стремится создать рабочее пространство для правозащитников в интересах социальной справедливости и соблюдения прав человека. В структуре ПБИ - международный Совет попечителей, международное представительство в Лондоне, региональные или ассоциированные группы в 17 странах. Организация также осуществляет целый ряд полевых проектов.

Европейский отдел «Пис Бригейдс Интернешнл» находится в Брюсселе (Бельгия). Материалы данного Пособия являются одним из результатов деятельности его Секции исследований и обучения.

Более подробные сведения о ПБИ вы найдете на ее официальном сайте
http://www.peacebrigades.org/

или на сайте ее Европейского отдела
http://www.peacebrigades.org/beo.html

Фонд «Фронт Лайн» был основан с предназначением направлять свою деятельность исключительно на защиту борцов за права человека. Достойно сожаления то обстоятельство, что каждый день нашей работы приносит все новые свидетельства необходимости усиления безопасности и защиты правозащитников в тех частях мира, где они все больше подвергаются риску. Основное внимание в нашей работе сосредоточено на усилении давления на правительства и на требовании их подотчетности, поскольку правительства, являясь субъектами международного законодательства о защите правозащитников, несут за неё прямую ответственность. Тем не менее, слишком часто они сами оказываются инициаторами репрессий против правозащитников. Однако, как явствует из свидетельств самих правозащитников, гораздо большего можно добиться путём улучшения их собственной системы безопасности.

Поэтому, когда мы узнали, что «Пис Бригейдс Интернешнл» разрабатывает проект под названием «Основные методы обеспечения безопасности», включавший в себя данное Пособие для правозащитников, нас это очень заинтересовало, и мы с готовностью согласились профинансировать их исследовательскую работу и издание настоящего Пособия.

Нам было приятно сотрудничать с автором этого руководства, Энрике Эгуреном. Вместе со своими коллегами, он привнес в наше работу свой богатый опыт в вопросах безопасности и защиты. Кроме того, сотрудники ПБИ организовали и провели ряд выездных семинаров с правозащитниками по месту их деятельности с целью опробовать данное Пособие и удостовериться, что оно действительно приносит пользу тем, кто трудится на «линии фронта». Два таких семинара были проведены совместно с Фондом «Фронт Лайн» в городах Букаву и Гома, Восточная Демократическая Республика Конго, в мае 2004 года.

Публикуя это Пособие, Фонд «Фронт Лайн» видит свою цель в обеспечении правозащитников практическим руководством , которое они могут использовать при разработке собственных планов и стратегий безопасности. Данная книга во многих своих аспектах представляет собой работу незавершенную и постоянно совершенствующуюся на основе опыта правозащитников, действующих во враждебной среде. Содержание книги значительно расширилось благодаря дискуссиям по проблемам безопасности и защиты во время 1-й и 2-й Дублинских Трибун правозащитников, проходивших в 2002 и 2003 годах. В программу 3-ей Дублинской Трибуны правозащитников в октябре 2005 года включена дискуссия по конкретным направлениям безопасности, а также рассмотрение отзывов на данное Пособие.

В настоящем Пособии предпринята попытка углубленного рассмотрения вопросов анализа степени риска и угроз, а также разработки действенных мер безопасности и защиты. Надеемся, что книга эта станет как полезным практическим пособием для ответственных за безопасность сотрудников правозащитных НПО, так и учебным пособием для обучения правозащитников. В наших замыслах – издание краткого практического справочника в дополнение к настоящему Пособию. Фонд «Фронт Лайн» в настоящее время - совместно с организацией «Приватерра» - разрабатывает специальное приложение к растоящему Пособию по проблеме электронной связи и компьютерной безопасности, которое планируется опубликовать в 2005 году. Эта проблема вкратце освещена в главе 12 настоящего Пособия.

Считаем своим долгом выразить признательность за содействие целому ряду лиц, без которых это Пособие не появилось бы на свет.

Работа Мэри Сарадж, Паскаль Бостан, Майкла Скулза и Кристофа Клотца,

дорогих коллег из Европейского отдела ПБИ, имела ключевое значение для этого проекта. Без их опыта и приверженности делу издание этой книги было бы невозможным.

Текст данного Пособия критически проанализирован и отредактирован Мери Лолор, Эндрю Андерсоном, Джеймсом Мехиганом и Дмитрием Витальевым (глава 12) – сотрудниками Фонда «Фронт Лайн». Первый вариант текста редактировала Кристин Хулаас Зунде.

Материалы главы 12 основаны на результатах работы Роберта Гуэрры, Катицы Родригес и Карин Мэдден из организации «Приватерра (Privaterra)», Канада.

Мы признательны за присланные материалы и замечания по рукописи, полученные от Арнольда Тсунга («Юристы Зимбабве за права человека»), Сихема Бенседрина (Национальный совет за свободы в Тунисе, Тунис), Отца Бендана Форде (Орден Странствующих францисканцев, Колумбия), Индаи Сахор (бывший директор Азиатского центра по правам женщин, Филиппины), Джеймса Кавальяро (первый помощник директора, Программа по правам человека, Гарвардская юридическая школа, Бразилия), Надежды Маркес (консультант и исследователь, «Глоубл Джастис Сентр», Рио-де-Жанейро, Бразилия) и Мери Сарадж (ПБИ ЕО, Бельгия).

Ряд коллег также сделал свой вклад. Мы не можем не упомянуть Хосе Круза и Идувину Эрнандес из организации SEDEM (Гватемала), Клаудиу Самайоа (Гватемала), Хайме Прието (Колумбия), Эмму Иствуд (Великобритания) и Синтию Лавандера, сотрудницу программы «Борцы за права человека», «Эмнисти Интернешнл», Лондон.

Кармен Диез Розас со всем тщанием разработала макет этого настоящего Пособия и напечатала оригинал-макет средствами настольной типографии, а Монсеррат Муньос консультировала в ходе печатных работ и оказала помощь в подготовке иллюстраций.

Мы также благодарны за оказанную поддержку организации «Девелопмент Коуперейшн Айрланд (Development Cooperation Ireland)».

Отпечатано компанией 'Принт энд Дисплей'.

(От автора) множество других людей внесли свой вклад в сбор данных , необходимых для написания настоящего Пособия. Невозможно перечислить всех, но хотелось бы упомянуть хотя бы некоторых, а именно:

всех сотрудников ПБИ, но особенно моих давних близких коллег по проекту «Колумбия» - Маргу, Элену, Франсиско, Эмму, Томаса, Хуана, Микеля, Сольвейг, Мирьям и многих-многих других...

Данило, Клеменсию и Абилио и их коллег из «Комисио Интерэклезиаль де Хустисио и Паз» в Колумбии. Они научили меня, как жить в сердцах людей.
Жителям деревень Санта-Мария в Сальвадоре и Какарика, Хигуамиандо и Сан-Хосе де Апартадо в Колумбии. Они, между прочим, являли собой образчики собственного достоинства.

Активным участникам программы по безопасности для правозащитников, организованной Консультативной службой проекта в Колумбии.

За советы и начальное обучение, предоставленные REDR (Лондон) и Конрадом ван Брабантом (Бельгия).

А также множеству правозащитников, встреченных в Сальвадоре, Гватемале, Колумбии, Мексике, Шри Ланке, Хорватии, Сербии, Косово, Руанде, Демократической Республике Конго, Ингушетии и т.д. Это были моря слёз и улыбок, бесед, познания и преданности делу ...

И, в заключение, эта книга не была бы написана без любви, преданности и поддержки со стороны Гризелы, Икер и моих родителей. Всю свою любовь отдаю им.

Мы благодарны всем, упомянутым выше, а также многим правозащитникам, с которыми мы работали и у которых многому научились. Однако за окончательную редакцию текста, а также за любую ошибку, которая могла вкрасться в него, общую ответственность несут «Фронт Лайн» и ПБИ. Мы надеемся, что это Пособие окажется полезным для улучшения защиты и безопасности правозащитников, хотя мы и сознаем, что оно не дает никаких гарантий. В конечном итоге, каждый человек должен быть в состоянии нести ответственность за себя. Ждём ваших отзывов, предложений и замечаний.

Фонд «Фронт Лайн»
«Пис Бригейдс Интернешнл»
7 марта 2005

Предупреждение

Содержание настоящего Пособия не обязательно отражает точку зрения «Пис Бригейдс Интернешнл» и «Фронт Лайн» (Международного фонда защиты борцов за права человека).

Ни авторы, ни издатель не гарантируют того, что сведения, содержащиеся в данной публикации являются полными и точными, и они снимают с себя всякую ответственность за любой ущерб, понесенный вследствие их использования. Ни одна из частей данного Пособия не может быть принята за норму или гарантию, либо использоваться без необходимого критерия оценки риска и проблем безопасности, с которыми может

Содержание

ПОСОБИЕ ДЛЯ ПРАВОЗАЩИТНИКОВ ПО ЗАЩИТЕ И БЕЗОПАСНОСТИ

Правозащитники в опасности

Хотя соблюдение прав человека и гарантируется международным законодательством, деятельность по обеспечению их реализации и рассмотрение их нарушений могут быть опасными в разнличных странах мира. Правозащитники часто оказываются единственной силой, стоящей между простыми людьми и неконтролируемой властью государства. Их деятельность жизненно необходима для развития демократических процессов и становления демократических институтов, для борьбы с безнаказанностью и защиты прав человека.

Правозащитники часто подвергаются притеснениям, арестам, пыткам.Они становятся жертвами клеветнических кампаний, их увольняют с работы, ограничивают свободу их передвижения и создают трудности в юридической регистрации их организаций. В некоторых странах они погибают либо бесследно "исчезают".

В течение последних нескольких лет возросла осведомленность широких кругов общественности относительно того огромного риска, с которым сталкиваются правозащитники в своей работе. Этот риск очень легко распознать, когда правозащитники работают во враждебной среде, например, в случае, когда законодательство какой-либо страны карает граждан за определенные виды правозащитной работы. Однако правозащитники рискуют даже тогда, когда законодательство, с одной стороны, без каких-либо ограничений санкционирует правозащитную работу, но с другой - не в состоянии наказать тех, кто угрожает правозащитникам или нападает на них. Во время вооруженных конфликтов этот риск неизмеримо возрастает.

За исключением тех редких случаев когда жизнь правозащитника может оказаться в руках солдат на контрольно-пропускном пункте, насилие, совершаемое в отношении правозащитников, не может квалифицироваться как случайное. В большинстве случаев, насильственные действия против них являются предумышленными, тщательно спланированными и продиктованными явными политическими либо военными соображениями.

Подобные ситуации требуют от правозащитников разработки и осуществления всеобъемлющей и динамиччной стратегии безопасности в их повседневной работе. Но одних лишь благих пожеланий или советов «соблюдать осторожность» явно недостаточно. Здесь требуется хорошо организованный контроль за собственной безопасностью. Данное Пособие не предлагает готовых рецептов, применимых к любому сценарию событий. Цель его – представить набор стратегий, направленных на улучшение системы контроля за безопасностью правозащитников.

Самые эффективные уроки безопасности исходят от самих правозащитниковю Они являются результатом их каждодневного опыта, а также тактики и стратегии по защите других лиц и их рабочей среды. Поэтому данное Пособие следует рассматривать как труд, пребывающий в постоянном процессе усовершенствования и – по мере получения откликов от правозащитков на переднем крае - требующий постоянного обновления и поправок.

Мы также можем многому поучиться у международных гуманитарных НПО, с недавнего времени разрабатывающих собственные правила и методы обеспечения безопасности своих сотрудников.

Важно осознавать , что главной опасностью для правозащитников является то, что угрозы часто ведут к реальному насилию над ними. У нападающих имеется желание, средства и сознание собственной безнаказанности для осуществления этих угроз. Поэтому наилучшее средство профилактики для правозащитников – это политические действия, вынуждающие правительства и гражданское общество оказывать давление на тех, кто постоянно угрожает жизни правозащитников, преследует и убивает их. Рекомендации, предлагаемые данным руководством, никоим образом не подменяют собой ответственность за защиту правозащитников каждого в отдельности и всех вместе взятых правительств мира.

Невзирая на всё сказанное выше, правозащитники могут существенно улучшить свою безопасность, следуя некоторым испытанным правилам и методам.

Данное Пособие представляет собой лишь скромный вклад в достижение цели, к которой стремятся множество различных организаций: сохранить в неприкосновенности ту неоценимую работу, которую ведут правозащитники. Они – бойцы с переднего края - и являются главными героями этой книги.

Пособие

Цель настоящего Пособия - вооружить правозащитников дополнительными знаниями и методами, которые могут оказаться полезными для более глубокого понимания системы безопасности и защиты. Надеемся, что данное руководство послужит подспорьем в обучении этим методам и поможет правозащитникам проводить собственные оценки риска и выбирать наиболее приемлемые правила и методы безопасности.

Данное Пособие является итогом долговременного проекта по защите правозащитников в оперативных условиях, осуществляемого ПБИ. При его составлении, мы использовали опыт и знания сотен правозащитников, встреченных нами как на местах, так и на семинарах, совещаниях и дискуссиях по вопросам безопасности. Большая часть материала, представленного в руководстве, применялась на практике - как в рельной деятельности по организации защиты, так и на учебных семинарах. Настоящее Пособие - результат этих обменов мнениями, и мы глубоко признательны всем правозащитникам, которые внесли в него свою лепту.

Безопасность и защита – очень сложные области. Они зиждятся на прочных знаниях, но в то же время подвержены воздействию соображений отдельных лиц и организаций. Осознание правозащитниками необходимости уделять проблемам безопасности должное время, внимание и энергию, невзирая на занятость, стресс и страх - одна из основных задач этой книги. А это означает выход за пределы индивидуальных знаний и продвижение в направлении организационной культуры, в которой безопасность будет понятием само собой разумеющимся.

Другими важными элементами эффективной безопасности являются глубокое знание сценария развития того или иного конфликта и понимание местной политической

логики. Настоящее Пособие обрисовывает как общий, так и постепенный подход к достижению эффективной безопасности. Оно также содержит замечания о таких важнейших понятиях, как риск, уязвимость и опасность, а также ряд предложений относительно того, как усовершенствовать и развивать систему безопасности для правозащитников в их повседневной работе. Надеемся, что все затронутые темы позволят НПО и правозащитникам планировать развитие систем безопасности и справляться с нарастающими в этой области проблемами, связанными с защитой прав человека.

Здесь нам представляется уместным напомнить о том, что правозащитники рискуют своим благополучием и самой жизнью, и это очень серьезно. Иногда, уход в подполье с последующим бегством - единственный способ спастись. Хотелось бы подчеркнуть, что все методики и предложения, изложенные в этой книге, ни в коей мере не являются исчерпывающими. Пособие написано добросовестно, но, как это ни печально, оно само по себе не дает гарантий на успех.

Давайте вместе улучшим это Пособие ...

Данное Пособие – труд незавершенный и со временем потребует улучшения. Отзывы правозащитников по любому аспекту этого Пособия будут приветствоваться.

Ждём ваших откликов и мнений, особенно о том, насколько полезным для вашей работы явилось настоящее Пособие. С вашей помощью мы попытаемся увеличить его полезность для правозащитников во всем мире.

Вы можете связаться с нами по электронной почте:

- protectionmanual@frontlinedefenders.org
- pbibeo@biz.tiscali.be

а также обратиться с письмом в ПБИ или в Фонд «Фронт Лайн» по адресу:

- PBI- European Office
  38, Rue Saint-Christophe, 1000 Bruxelles (Belgium)
  тел./факс: + 32 (0)2 511 14 98

- Front Line
  16 Idrone lane, Off Bath Place, Blackrock, County Dublin, Ireland
  тел.: +353 1212 3750; факс: +353 1212 1001

Кто такие «защитники прав человека»?

«Защитник прав человека» - это термин, используемый для описания людей, которые самостоятельно, либо коллективно, предпринимают действия для обеспечения или защиты прав человека. Таким образом, защитников прав человека (либо –«правозащитников») можно определить, прежде всего, по виду их деятельности, и, стало быть, данное понятие может быть наиболее точно охарактеризовано путём описания их действий, а также среды, в которой они работают.

В 1998 году Генеральная Ассамблея Объединенных Наций утвердила «Декларацию о праве отдельных лиц, общественных групп и организаций обеспечивать и защищать общепризнаные права и основные свободы человека и их ответственности за это» (далее – «Декларация ООН о правозащитниках»). Иными словами, спустя пятьдесят лет после принятия Всеобщей Декларации о правах человека и через двадцать лет после переговоров о проекте декларации о правозащитниках, ООН, в конце концов, признала, что тысячи людей во всём мире так или иначе вовлечены в защиту прав человека. Эта всеобъемлющая Декларация отдаёт должное масштабам и многогранности деятельности по защите человеческих прав.

Специальный представитель Генерального секретаря ООН по правам человека имеет полномочия «изыскивать, получать и проверять сведения о состоянии прав отдельных лиц либо групп людей, а также реагировать на них с целью обеспечения защиты прав и основных свобод человека».

Фонд «Фронт Лайн» характеризует защитника прав человека как «лицо, борющееся ненасильственными методами за соблюдение отдельно взятых либо всех в совокупности прав, закрепленных во Всеобщей Декларации ООН о правах человека». «Фронт Лайн» призывает к неукоснительному соблюдению Декларации ООН о правозащитниках (см. полный текст этой Декларации на с. 113).

Кто ответственен за защиту правозащитников?

Декларация о правах человека подчеркивает, что, за защиту правозащитников отвечает, прежде всего, государство. Она также признает «ценный вклад отдельных лицв, групп и ассоциаций в деятельность по искоренению нарушений прав и основных свобод человека», а также «взаимосвязь между миром и безопасностью и осуществлением прав и основных свобод человека».

Как заявила специальный представитель Генерального секретаря ООН по правам человека Хина Джилани, «вскрытие случаев нарушения прав человека и поиски путей их устранения во многом зависят от степени безопасности самих правозащитников»[1]. Пытки, исчезновения, убийства, угрозы, ограбления, взломы рабочих помещений, преследования, незаконные аресты, давление со стороны секретных служб, полицейский надзор и т.п. неизменно фигурируют в каждом отчете о положении правозащитников в мире. К сожалению, подобное положение правозащитников является правилом, а не исключением.

[1] Доклад о правозащитниках, 10 сентября 2001 г. (A/56/341).

Рекомендуемые материалы для изучения

Если вы желаете расширить ваши знания о правозащитниках, посетите следующие вебсайты:

- Верховный Комиссар ООН по правам человека (the UN High Commissioner for Human Rights): www.unhchr.ch/defender/about1.htm

- «Фронт Лайн», Международный фонд защиты борцов за права человека, Ирландия (Front Line - The International Foundation for the Protection of Human Rights Defenders): www.frontlinedefenders.org

- www.peacebrigades.org/beo.html (The European Office of Peace Brigades International in Brussels).

- Наблюдательная комиссия по защите правозащитников (The Observatory for the Protection of Human Rights Defenders), создана Международной Федерацией по правам человека (International Federation on Human Rights; FIDH; www.fidh.org) и Всемирной организацией против пыток (World Organisation Against Torture; OMCT; www.omct.org).

- «Международная Амнистия» (Amnesty International): www.amnesty.org и http://web.amnesty.org/pages/hrd-index-eng

- «Защита прав человека» Женева, Швейцария, искать под аббревиатурой "HRDO" (The HRD Office of the International Service for Human Rights): www.ishr.ch

- «Права человека прежде всего» (Human Rights First): www.humanrightsfirst.org

- «Фонд неотложных действий по правам женщин» (Urgent Action Fund for Women's Human Rights): www.urgentactionfund.org

Чтобы узнать больше о существующих правовых инструментах Декларации ООН о правозащитниках, посетите сайты:

- www.unhchr.ch : это сайт Верховного Комиссара ООН по правам человека

- www.frontlinedefenders.org/manual/en/index.htm : сайт Фонда «Фронт Лайн», Ирландия, содержит пособие по международному законодательству о правозащитниках и ссылки на другие сайты. см.: http://www.frontlinedefenders.org/links/

- www.ishr.ch/index.htm : на сайте Международной службы по правам человека, Женева (International Service for Human Rights) вы найдёте сводку материалов по международным и региональным законоположениям относительно защиты борцов за права человека.

Принятие обоснованных решений по безопасности и защите

Цель

Осознать важность анализа своей рабочей среды исходя из соображений безопасности.

Изучить различные методы проведения анализа обстановки и вовлечённых сторон.

Среда работы правозащитников

Защитники прав человека обычно трудятся в сложной среде, где действует множество различных персонажей , и которая находится под воздействием сугубо политических процессов принятия решений. Множество событий происходят почти что одновременно, причем каждое оказывает воздействие на другое. Динамика каждого персонажа либо заинтересованной стороны в этом сценарии играет значительную роль в их взаимоотношениях. Поэтому защитникам прав человека требуются сведения не только по вопросам, непосредственно связанным с их работой, но и о положении ключевых персонажей и вовлечённых сторон.

В качестве простого упражнения можно организовать коллективный «мозговой штурм» в попытке определить всех социальных, политических и экономических персонажей, способных влиять на текущую ситуацию с точки зрения вашей безопасности.

Анализ вашей рабочей среды

Очень важно как знать и понимать окружение, в котором вы работаете. Хороший анализ этого окружения дает возможность принимать обоснованные решения о том, какие правила и методы безопасности следует использовать. Также важно продумывать возможные будущие сценарии на предмет принятия превентивных мер.

Простой анализ рабочей среды, тем не менее, не является достаточным. Необходимо также думать о том, каким образом та или иная враждебная акция может воздействовать на ситуацию и как прореагируют на неё прочие персонажи. Не менее существенно также принимать во внимание масштабы подобного рабочего сценария. Его можно рассматривать на уровне **макродинамики**, т.е. изучая страну или целый регион, однако при этом следует уяснить, каким образом факторы макродинамики

действуют в вашем конкретном регионе, переходя таким образом на уровень **микродинамики.** Например, военизированные группировки в каком-либо регионе могут действовать не так, как можно было бы ожидать из анализа, предпринятого на местном либо национальном уровне. Необходимо быть осведомленным о подобных локальных вариациях. Не менее важно также избегать общепринятых воззрений на тот или иной рабочий сценарий, поскольку ситуации постоянно развиваются и меняются, и их необходимо время от времени пересматривать.

Тремя полезными методами анализа вашей рабочей среды являются: **Формулирование вопросов, Анализ силового поля и Анализ заинтересованных сторон:**

Формулирование вопросов

Постановка корректных вопросов относительно вашей рабочей среды поможет вам лучше разобраться в ней. Этот приём удобен для небольших дискуссий, однако лишь в том случае, если сама формулировка этих вопросов способствует принятию правильного решения.

Предположим, например, что притеснения со стороны местных властей переросли в серьёзную проблему. Если поставить вопрос так: «Что следует сделать для того, чтобы уменьшить притеснения?», то это значит, что вы ищете средства избавления всего лишь от отдельного симптома, в данном случае, притеснений, а не самой болезни.

Но если вы сформулируете проблему, делая акцент на её решении, то вы будете на верном на пути. Например, если вы спросите: «Достаточно ли безопасна социально-политическая среда для нашей работы?», то на такой вопрос возможны лишь два ответа – «да» или «нет».

Если «да», то следует сформулировать следующий вопрос, который поможет вам установить и правильно понять насущные проблемы поддержания вашей безопасности. Если после надлежащего рассмотрения всех видов деятельности, планов и ресурсов, а также законодательства, переговоров, сравнений с другими правозащитниками региона и т.п. последует ответ «нет», то это само по себе будет равнозначным решению проблемы.

Использование метода постановки вопросов:

- Ищите вопросы, которые помогут вам установить и правильно понять насущные проблемы поддержания вашей безопасности.
- Формулируйте вопросы таким образом, чтобы они подсказывали ответы
- Повторяйте этот процесс (как обсуждение) до достижения результата.

Примеры уместных вопросов:

- Какие проблемы в социально-политической и экономической сферах сейчас актуальны?
- Каких позиций по отношению к этим проблемам придерживаются основные заинтересованные стороны?
- Каким образом наша работа могла бы повлиять - негативно либо позитивно - на интересы основных заинтересованных сторон?
- Как нам следовало бы реагировать, если бы в результате нашей работы мы стали мишенью одного из этих персонажей?

- Достаточно ли безопасна наша социально-политическая среда для проведения нашей работы?

- Как реагировали местные/национальные власти на предшествующую деятельность правозащитников в данной сфере?

- Как реагировали основные заинтересованные стороны на предшествующую или сходную деятельность правозащитников или иных лиц в данной области?

- НКак в подобных обстоятельствах реагировали средства массовой информации и общество в целом?

- и т.п.

Анализ силового поля

Анализ силового поля представляет собой методику, которая может помочь в визуальной идентификации того, как различные силы способствуют или препятствуют достижению ваших целей. Эта методика позволяет выявить как силы поддержки, так и силы сопротивления, и исходит из допущения, что проблемы безопасности исходят в основном от сил сопротивления, в то время как силы поддержки действуют вам на пользу. Этот подход может практиковаться одним человеком, но становится наиболее эффективным, когда берётся на вооружение группой лиц с четко обозначенными целями и методами их достижения.

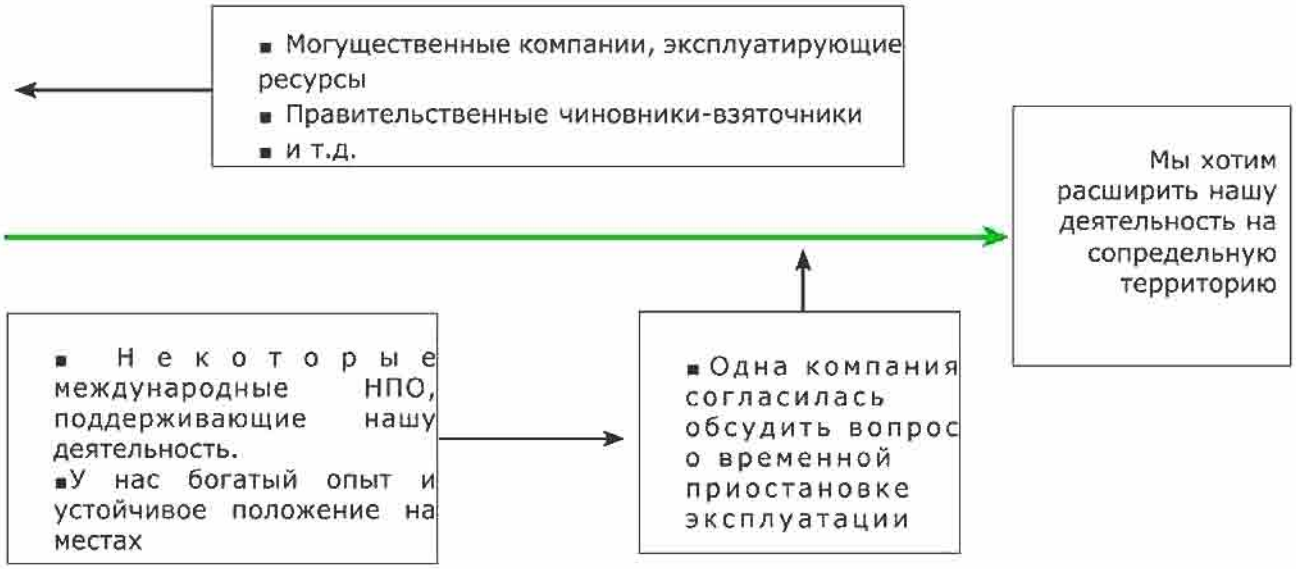
Начертите горизонтальную стрелку, направленную на блок. Впишите в него основные параметры той цели, к которой вы стремитесь. Это даст вам возможность сосредоточить внимание на идентификации сил поддержки и сопротивления. Нарисуйте еще один блок над центральной стрелкой. Перечислите в нем все потенциальные силы, которые могли бы помешать вам в достижении поставленной цели. Нарисуйте на схеме, ниже центральной стрелки, такой же блок, в котором перечислите все потенциальные силы поддержки. В последнем блоке укажите силы, направленность действия которых неизвестна либо неясна.

Схема 1: Анализ силового поля для оценки рабочей среды

По завершению блок-схемы, оцените полученные результаты. Анализ силового поляпозволяет вам чётко представить себе силы, с которыми вам приходится иметь дело.Задача заключается в том, чтобы найти пути снижения либо искоренения риска,порождаемого силами сопротивления, с помощью сил поддержки. Что касается силнеизвестной направленности, то следует решить, рассматривать ли их как подспорье либо продолжать наблюдать за ними с целью выявления их направленности (в сторону сопротивления либо поддержки).

Например:

Представим, что вы принадлежите к организации, занимающейся правами коренных жителей страны/региона на их природные ресурсы. Наблюдаются текущие конфликты между рядом заинтересованных сторон относительно использования этих ресурсов. Теперь вы хотите расширить вашу деятельность на сопредельный регион со сходными проблемами.



Анализ участников (или заинтересованных сторон)

Анализ участников (персонажей), либо заинтересованных сторон – один из важных путей повышения степени информированности в ходе принятия решений по безопасности и защите. Он включает идентификацию и описание различных участников или заинтересованных сторон, вовлеченных в процесс, и их взаимосвязей на основе их характеристик и интересов применительно сугубо к данной конкретной проблеме защиты.

Сторона, заинтересованная в защите – это любой лицо, группа лиц либо организация, заинтересованная либо вовлеченная в политику по достижению определённого результата в области защиты[1].

Ключом к пониманию вышесказанного является анализ заинтересованных сторон, а именно

- Кто является заинтересованными сторонами и при каких обстоятельствах с ними нужно считаться ?
- Каковы взаимосвязи между сторонами, заинтересованными в защите? Каковы их характеристики и интересы?
- Как повлияет на них деятельность по защите?
- Налицо ли готовность каждой заинтересованной стороны быть вовлеченной в деятельность по защите?

1 Выдержка из: Sustainable Livelihoods Guidance Sheets No. 5.4 (2000); адаптировано.

Стороны, заинтересованные в защите, можно категоризировать следующим образом:

Первичные заинтересованные стороны. В контексте защиты это сами правозащитники, а также те лица, которые работают с ними и на них, поскольку все они имеют первичный интерес в своей собственной безопасности (защите).

Заинтересованные стороны, ответственные за защиту правозащитников, при исполнении ими своих служебных обязанностей как например:

- Правительственные и государственные институты (включая силы безопасности, судей, сотрудников законодательных органов и т.д.)

- Международные организации, имеющие полномочия осуществлять защиту, такие как некоторые органы ООН, региональные межправительственные организации (МПО), миротворческие силы и т.п.

- При наличии персонажей вооруженной оппозиции, их можно рассматривать несущими ответственность за предотвращение нападений на правозащитников (поскольку последние относятся к гражданскому населению), особенно в том случае, когда эти персонажи контролируют определённую территорию.

Ключевые заинтересованные стороны, способные существенно влиять на защиту правозащитников. Они могут иметь политическое влияние или способность оказывать давление на заинтересованные стороны, не исплняющие надлежащим образом свои служебные обязанности (а именно – иные правительства, органы ООН, подразделения Международного комитета Красного Креста и т.д.). Подобным же образом некоторые из них могут быть прямо или косвенно вовлечены в нападения и оказание давления на правозащитников (такие как частные корпорации, средства массовой информации либо правительственные органы). Все зависит от контекста, интересов и стратегий каждой из вышеобозначенных основных заинтересованных сторон. Далеко не исчерпывающийся их перечень может включать:

- Органы ООН (кроме специально уполномоченных).
- Международный комитет Красного Креста (МККК, ICRC).
- Прочие правительства и многопрофильные организации (как финансирующие, так и директивные).
- Прочие вооруженные персонажи
- НПО (как национальные, так и международные).
- Церкви и религиозные организации.
- Частные корпорации.
- Средства массовой информации.

Главная трудность в определении стратегий и действий, к которым прибегают заинтересованные стороны, заключается в том, что взаимоотношения между ними проявляются неотчетливо, или даже могут вовсе не существовать. Многие заинтересованные стороны при исполнении служебных обязанностей, в частности правительства, силы безопасности и вооруженные силы оппозиции, либо принимают непосредственное участие в нарушениях прав человека и снижение степени защиты правозащитников, либо способствуют таковым. Некоторые заинтересованные стороны, которые могли бы при иных обстоятельствах разделять озабоченность относительно защиты, могут также иметь противоречащие друг другу интересы (что нередно происходит с прочими правительствами, органами ООН и НПО). Эти факторы, вместе с присущими конфликтам сценариями, усложняют картину рабочей среды как таковой.

ААНАЛИЗ ИЗМЕНЯЮЩИХСЯ СТРУКТУР И ПРОЦЕССОВ

Заинтересованные стороны не являются статичными персонажами. Они взаимодействуют друг с другом на многочисленных уровнях густой паутины взаимосвязей. С позиций защиты, очень важно уделять внимание взаимоотношениям, формирующим и преобразующим потребность людей в защите, предварительно чётко их определив. После чего мы сможем говорить о **структурах и процессах.**

Структуры представляют собой взаимосвязанные составные части государственного сектора, гражданского общества или частных организаций. Посмотрим на них с точки зрения защиты. Внутри государственного сектора правительство можно рассматривать как совокупность персонажей либо с одной общей стратегией, либо с внутренними взаимопротиворечащими тенденциями. Например, можно обнаружить существенные разногласия между министерством обороны и министерством иностранных дел, или между ведомством омбудсмана и военными при обсуждении политических проблем, связанных с деятельностью правозащитников. Структуры могут иметь смешанные компоненты; например, может быть создана межведомственная комиссия (членами которой будут представители правительства, НПО, ООН и дипломатического корпуса), которая будет тщательно следить за ситуацией с безопасностью данной организации правозащитников.

Процессы – это совокупность решений и действий одной или нескольких структур, направленные на улучшение ситуации с защитой данной группы. Процессы могут быть правоохранительными , культурными и политическими. Не все они успешны в достижении улучшененной защиты: во многих защитные процессы противоречат либо друг другу либо делают друг друга неээффективными. Например, люди, якобы находящиеся под защитой, могут не соглашаться с правительственной политикой по данному вопросу, поскольку видят, что этот политический процесс скрыто направлен на перемещение населения из из данного местности. ООН и неправительственные организации могут поддержать людей во время данного процесса.

Существует ряд способов проведения анализа заинтересованных сторон. Способ, описанный ниже, использует простую методологию, позволяющую получать хорошие результаты в процессах анализа и принятия решений.

При оценке процессов защиты важно рассматривать их в адекватной временной перспективе и всегда учитывать интересы и цели всех заинтересованных сторон.

Четыре Этапа анализа заинтересованных сторон:

1. • Определите вопрос защиты более широко (т.е. какова ситуация с безопасностью правозащитников в данном регионе страны).

2. • Кем являются заинтересованные стороны? (А именно, какие организации, группы и отдельные лица отвечают за безопасность либо заинтересованы в защите?) Определите и назовите – с помощью «мозговых штурмов и дискуссий - все заинтересованные стороны, имеющие отношение к данному вопросу защиты.

3. • Исследуйте и проанализируйте характеристики заинтересованных сторон и их отдельные признаки, такие как ответственность за защиту, сила влияния нанеё, цели, стратегии, легитимность и интересы (включая желание внести вклад в дело защиты).

4. • Исследуйте и проанализируйте взаимосвязи между заинтересованными сторонами.

По завершение этого анализа, вы можете воспользоваться матрицей, подобной приведенной ниже.

Поместите в матрице перечень всех заинтересованных сторон, имеющих отношение к строго очерченному вопросу защиты (Схема 2) : скопируйте его в первой колонке - как по вертикали так и по горизонтали. После этого можно провести два типа анализа:

- Для того, чтобы проанализировать признаки каждой заинтересованной стороны (ее цели и интересы, стратегии, легитимность и власть), заполните ячейки, расположенные по диагонали, где пересекаются наименования одних и тех же заинтересованных сторон.

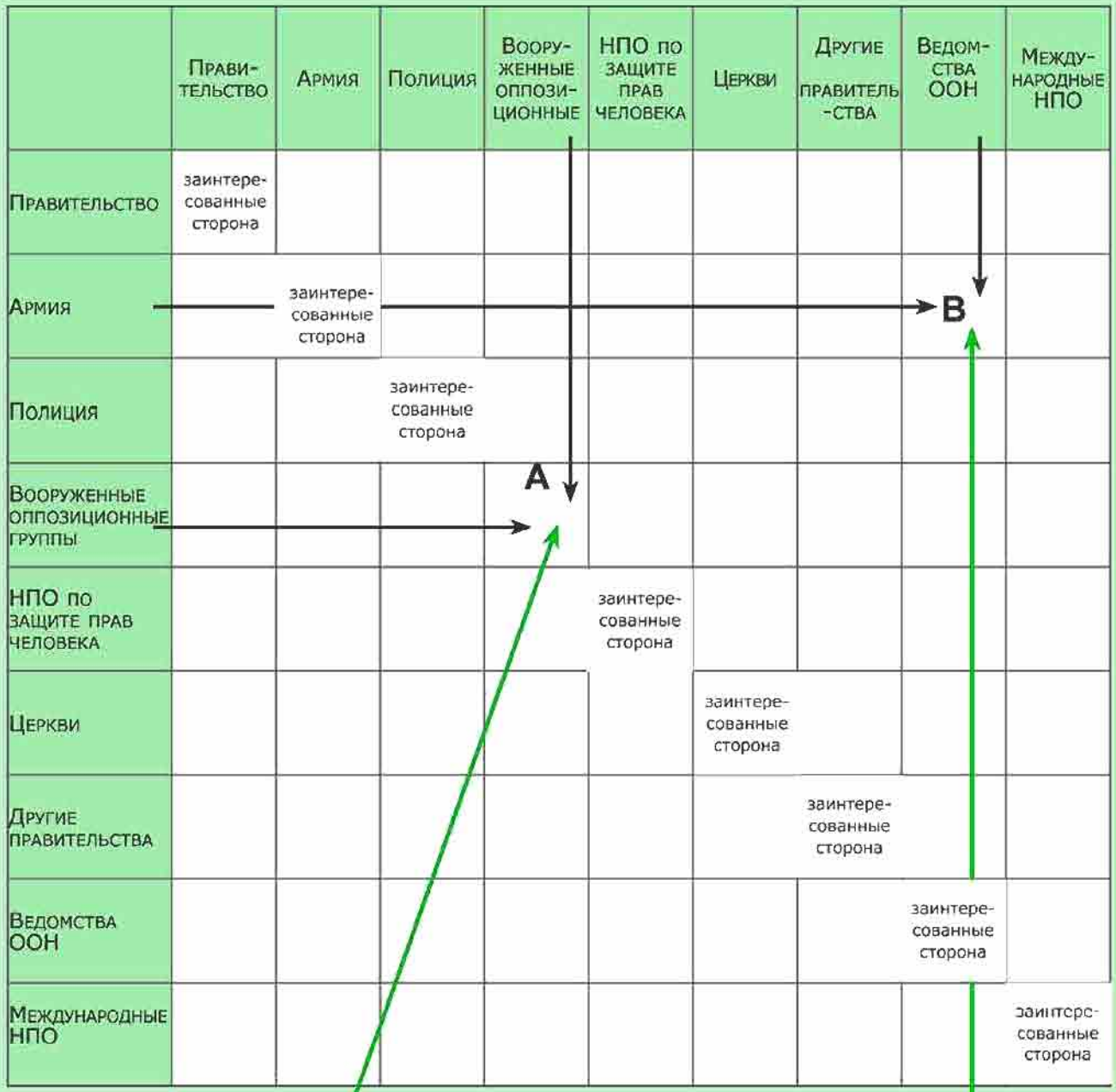
Например:

Можно поместить цели, интересы и стратегии формирований вооруженной оппозиции в ячейку "А".

- Для того, чтобы проанализировать взаимосвязи между заинтересованными сторонами, заполните те ячейки, которые отражают наиболее важные из них в вопросах защиты, например, точку пересечения колонок вооружённых сил страны с Верховного Комиссара ООН по делам беженцев (ВКОНДБ; UNHCR) в ячейке «В» и т. д.

После заполнения наиболее значимых ячеек, вы получите общую картину целей, стратегий и взаимодействий между основными заинтересованными сторонами по отношению к данному вопросы защиты.

Схема 2: Матрица для анализа заинтересованных сторон



Ячейка «А»

Для каждой заинтересованной стороны:
цели и интересы
стратегии
легитимность
власть

Ячейка «В»

Взаимосвязь между заинтересованными сторонами: (взаимосвязи по вопросам защиты и стратегии для обеих заинтересованных сторон)

ОЦЕНКА РИСКА: УГРОЗЫ, УЯЗВИМЫЕ МЕСТА И РЕСУРСЫ

Цель

Понимание концепций угрозы, уязвимости и ресурсов обеспечения безопасности.

Изучение методов оценки риска.

Анализ риска и требования защиты

Работа правозащитников может наносить ущерб интересам отдельных персонажей и это, в свою очередь, может поставить правозащитников под угрозу. Поэтому важно подчеркнуть, что **в отдельных странах риск является неотъемлемой частью жизни правозащитников.**

Проблему риска можно рассматривать следующим образом:

> Анализ интересов и стратегий основных действующих лиц ⇨ Оценка влияния работы правозащитников на эти интересы и стратегии ⇨ Оценка угроз в адрес правозащитников ⇨ Оценка уязвимых мест и ресурсов правозащитников ⇨ Определение риска.

Другими словами, работа, которую вы выполняете в качестве правозащитника, может повысить степень риска с которым вы сталкиваетесь.

- **Ваша работа** может привести к появлению угроз.
- Степень вашей уязвимости зависит от того, **как, где** и **когда** вы работаете.

Общепринятого определения понятия «риск» не существует, но мы можем сказать, что под риском можно понимать возможные события, пусть и не вполне определённые, в результате которых наносится ущерб.

Каждый правозащитник, как правило, испытывет некий общий уровень опасности, однако не все лица, пребывающие в одном и том же месте, одинаково уязвимы. **Уязвимость**, то есть возможность того, что правозащитник или группа таковых подвергнется нападению или понесёт ущерб, меняется, как мы увидим ниже, в зависимости от нескольких факторов.

Пример:

Можно найти страну, в которой правительство представляет общую угрозу для любой работы по защите прав человека. Это означает, что риск существует для всех правозащитников. Но мы также знаем, что некоторые правозащитники рискуют больше, чем другие; например: большая хорошо организованная НПО (неправительственная организация), базирующаяся в столице, вероятно, не столь уязвима, как маленькая местная НПО. И хотя, с точки зрения здравого смысла, вышесказанное не вызывает вопросов, для лучшего понимания проблем безопасности правозащитников было бы интересно проанализировать, почему это происходит.

Уровень риска, с которой сталкивается группа правозащитников, возрастает в соответствии с полученными угрозами и их уязвимостью перед ними, как представлено в уравнении[1] ниже:

РИСК = УГРОЗЫ X УЯЗВИМЫЕ МЕСТА

Угрозы представляют собой возможность того, что кто-то причинит физический или моральный ущерб кому-то или его имуществу путем преднамеренных и зачастую насильственных действий[2]. Оценка угрозы означает анализ вероятности её осуществления

При развитии событий по конфликтному сценарию, правозащитники могут сталкиваться с различными угрозами, включая конкретные и непосредственно ни них направленные, неконкретные, а также угрозы, исходящие от общего преступного элемента той или иной страны.

Наиболее распространенные из них - **направленные угрозы** - имеют целью помешать деятельности группы, либо изменить её, а также – оказать давление на её членов. Направленные угрозы обычно тесно связаны с работой конкретных правозащитников, а также с интересами и потребностями людей, стремящихся ей воспрепятствовать.

Правозащитники могут столкнуться **с угрозой обычных криминальных нападений**, особенно в тех случаях, когда их деятельность осуществляется в зонах повышенного риска. Причём, направленные угрозы зачастую пытаются выдать за ом «обычные» криминальные инциденты.

Скрытые угрозы происходят из вероятности потенциально ущерба в результате боевых действий в зонах вооруженных конфликтов и, как правило, представляют собой несчастные случаи.

Направленные угрозы можно также рассматривать по иному – в тех случаях , когда правозащитники имеют дело **сдекларированным** запугиванием, как например: при получении

Краткий список видов угроз/ опасностей:

- Направленные угрозы (сдекларированные угрозы, потенциальные угрозы): опасности связанные с вашей деятельностью
- Угрозы обычных криминальных нападений
- Скрытые угрозы: угрозы связанные с участием в вооруженных конфликтах

1 Van Brabant (2000) and REDR.

2 Dworken (1999).

угрозы убийства (см. Главу 3, оценка декларированной угрозы). Существуют также **потенциальные** угрозы, когда угрожают вашему коллеге-правозащитнику, и есть основания считать, что вы станете следующей мишенью.

Уязвимые места

Уязвимость означает степень, в которой люди чувствительны к убыткам, ущербу, страданиям и смерти в случае нападения. Она различна у каждого правозащитника и у каждой группы и меняется с течением времени. Уязвимость всегда относительна, так как все люди и группы в определенной степени уязвимы. Тем не менее, в зависимости от обстоятельств, у каждого имеется свой уровень и тип уязвимости. Давайте рассмотрим несколько примеров:

- Уязвимость может быть связана с местонахождением. Например: правозащитник обычно более уязвим, когда он/она находится на пути к месту событий, чем в офисе, где, в случае нападения, скорее всего, будут очевидцы.

- Уязвимыми местами могут быть те, где отсутствует доступ к телефону, к безопасному общественному транспорту, а также дома без надежных дверных замков. Уязвимость также увеличивается при отсутствии надлежащих механизмов связи между правозащитниками.

- Уровень уязвимости и страха также соотносится с тем, работает ли правозащитник в одиночку либо в составе группы коллег. Получивший угрозу, он.она может испытывать чувство страха, которое будет влиять на его/ее работу. Если у него/неё нет способа избавиться от этого страха (поговорить с кем-нибудь, пообщаться с группой своих коллег), то возникает вероятность ошибок либо принятия неверных решений, которые могут привести его/её к ещё большим проблемам в области безопасности.

(В конце этой главы приведен сводный перечень возможных уязвимых мест и ресурсов ащиты).

Ресурсы

Ресурсы защиты - это силы и средства, которыми группа или отдельный правозащитник могут воспользоваться для достижения разумной степени безопасности. Примерами могут служить: обучение по проблемам безопасности или по юридическим вопросам, коллективные и координированные действия, доступ к телефону и безопасному транспорту и налаженная связь с группами коллег-правозащитников, а также – умение совладать с чувством страха и т.д.

В большинстве случаев уязвиммые места и и ресурсы защиты являются двумя сторонами одной и той же монеты.

Например:

Отсутствие достаточной информации о вашей рабочей среде - это уязвимое место, а наличие этой информации – ресурс защиты. То же самое можно сказать и о наличии/отсутствии доступа к безопасному транспорту или к группам колллег-правозащитников.

(В конце этой главы приведен сводный перечень возможных уязвимых мест и ресурсов защиты).

Риск, порождаемый угрозами и уязвимыми местами, может быть снижен, если правозащитники обладают достаточными ресурсами (чем больше ресурсов, тем меньше риск).

$$\text{Риск} = \frac{\text{угрозы} \times \text{уязвимые места}}{\text{ресурсы}}$$

Заключение:

Для снижения риска до приемлемого уровня - а именно, для обеспечения защиты – вам следует:

- Уменьшить число/частоту угроз.
- Уменьшить факторы уязвимости
- Увеличить защитные ресурсы.

Риск – это динамичное понятие, которое меняется со временем и с изменением характера угроз, уязвимых мест и ресурсов. Это означает, что риск необходимо периодически переоценивать, особенно при изменении условий вашей работы, уязвимых мест и ресурсов. Например: уязвимость может возрасти, если в результате смены руководства положение группы правозащитников оказывается более слабым, чем ранее. Риск резко возрастает при появлении реальной и очевидной угрозы. В таких случаях попытки снижения риска путем расширения ресурсов защиты небезопасны, поскольку для этого требуется время.

Меры безопасности, такие как юридическая подготовка или защитные барьеры, могут снизить риск вследствие сокращению факторов уязвимости. Однако эти меры не устраняют главный источник риска, то есть угрозы и намерения их осуществления, особенно в ситуациях, когда преступники знают, что они, скорее всего, останутся безнаказанными. Таким образом, все основные изменения мер защиты должны быть направлены на уменьшение числа угроз, равно как и на снижение уязвимости и усиление ресурсов защиты.

Пример:

Небольшая группа правозащитников занимается проблемами земельной собственности в каком-либо городе. Когда их работа начинает затрагивать интересы местного землевладельца, они получают неприкрытую угрозу убийства. Если применить уравнение риск к данной ситуации, то вы увидите, что риск, с которым столкнулись эти правозащитники, очень высок, особенно из-за угрозы убийства. Если вы хотите снизить риск, то в данный момент ни замена замков на двери их офиса (поскольку риск не связан со взломом офиса), ни приобретение сотового телефона для каждого участника группы (хотя связь и является важным элементом безопасности), не будет достаточным, если появится убийца). В этом случае для прямого устранения угрозы более правильной стратегией было бы сделать эти угрозы достоянием гласности и вызвать политический резонанс (а если это вряд ли удастся осуществить в сжатые сроки, то единственным способом существенного уменьшения риска будет снижение общественной активности самих правозащитников, или, скажем, временное перемещение их офиса в другое место, ибо возможность переезда в более безопасное место также является ресурсом защиты).

Уязвимые места и ресурсы защиты, равно как и некоторые угрозы, могут варьироваться в зависимости от пола и возраста правозащитников, и это тоже неоходимо принимать во внимание.

Оценка уязвимых мест и ресурсов защиты

Расчет оценки уязвимости и ресурсов защиты для той или иной группы (либо для одного) подразумевает определение самой группы (общины, коллектива, НПО, отдельных лиц и т.д.), а также – географического региона, в котором он/она.они пребывает/ют и временной линии (характер вашей уязвимости будет изменяться и эволюционировать с течением времени). После этого, пользуясь **схемой 3** в конце этой главы как руководством, вы можете перейти к оценке уязвимых мест и ресурсов защиты.

Помните: Оценка уязвимых мест и ресурсов должна рассматриваться как непрерывный процесс, направленный на сбор имеющейся информации для получения точной картины постоянно меняющейся ситуации. При оценке ресурсов защиты важно определить реальные, т.е. существующие на данный момент, ресурсы, а не ресурсы потенциальные либо желаемые.

Стратегии преодоления риска и реагирования на него

Правозащитники и группы, находящиеся под угрозой, используют различные **стратегии преодоления риска**, с которым они сталкиваются. Эти стратегии в значительной степени изменяются в зависимости от окружающей среды (сельская, городская), вида угрозы, имеющихся в наличии социальных, финансовых и юридических ресурсов и т.д.

Большинство стратегий преодоления риска можно осуществлять быстро и целенаправленно. Поэтому они являются скорее тактическими приемами, а не детально разработанными стратегиями реагирования. Большинство таких стратегий преодоления находятся в соответствии с субъективным восприятием риска отдельными людьми и иногда могут нанести группе в целом определенный ущерб, в особенности если остановить их развитие не представляется возможным.

Стратегии преодоления риска тесно связаны с природой и степенью серьезности угрозы, а также с ресурсами и уязвимыми местами той или иной группы.

Думая о безопасности и защите, вы должны учитывать не только свои, но и чужие стратегии преодоления. Смело внедряйте наиболее эффективные из них, отвергая те, которые не сработали, и при этом не забывайте о тех, что остаются в запасе (в особенности о тех, что связаны с культурой и религией).

Некоторые типичные стратегии преодоления риска:

- Укрепление защитных барьеры и укрытиеценностей .
- Стремление избегать действий, с которыми может не согласиться другой персонаж, особенно в районах вооружённых конфликтов.
- в случае опасности – поиск убежища в труднодоступных местах – таких как как горы либо джунгли, смен места проживания и т.д. Иногда прячется лишь сам правозащитник, но порою в укрытие - под покровом ночной темноты - уходят целыми семьями и остаются там в течение нескольких недель, избегая контактов с окружающим миром.
- Обращение за военной либо политической защитой к одному из вооружённых персонажей.
- Приостановление работы, закрытие и эвакуация офиса. Перезд другой район страны, либо за границу.
- Упование на «удачу» либо на «добрые приметы".
- Скрытность и нелюдимость, в том числе и в отношениях с коллегами; отрицание реальности угроз, отказ от их обсуждения; пьянство, работа в сверхурочные часы, непредсказуемые поступки.

Правозащитники могут также воспользоваться такими стратегиями реагирования как выпуск соответствующих досье, публичные обвинения, организация демонстраций и т.д. Во многих случаях, эти стратегии не становятся долгосрочными, а служат лишь для решения насущных вопросов. В некоторых случаях, стратегии реагирования могут привести к ещё большим проблемам безопасности, чем те, которые они были призваны решить изначально.

При анализе стратегий преодоления риска и реагирования учитывайте следующее:

- Способность к быстрому реагированию: Могут ли ваши стратегии быстро отреагировать на проблемы отдельного лица или группы людей?

- Приспособляемость: Могут ли ваши стратегии быстро приспособиться к новым условиям, когда риск нападения уже позади? Правозащитник может иметь несколько вариантов выбора, например: либо самому скрываться либо жить некоторое время в домах других людей. Такие стратегии могут показаться слабыми либо нестабильными, но зачастую они оказываются очень надежными.

- Устойчивость: Могут ли ваши стратегии выдержать испытание временем, несмотря на угрозы или нападения без летального исхода?

- Эффективность: Могут ли ваши стратегии адекватно защитить отдельных людей или группы лиц, над которыми нависла угроза?

- Реверсивность: Если ваши стратегии не дают результата или изменяется ситуация, можно ли их изменить либо повернуть вспять?

Действия после оценки риска

После оценки риска вам необходимо проанализировать полученные результаты. Так как «размеры» риска с которым вы столкнулись точно определить невозможно, вам необходимо ввести такое понятие, как **уровень** риска.

Различные правозащитники и организации могут по-разному оценивать уровни риска. То, что неприемлемо для одних правозащитников, может быть приемлемо для других, то же самое можно сказать в отношение сотрудников одной и той же организации. Вместо того, чтобы обсуждать что именно «необходимо» сделать и готовы ли вы к этому, нужно принять во внимание тот факт, что у различных людей могут быть разные пороги риска, и вам предстоит найти общеприемлемый порог для всех них.

Исходя из вышеизложенного, на риск можно реагировать по-разному:

- Вы можете **принять** риск как данность, поскольку считаете, что сможете с этим жить.

- Вы можете **снизить** риск путем противодействия угрозам, сужения уязвимых мест и расширения способностей к защите.

- Вы можете **разделить** риск путем проведения совместных акций с другими правозащитниками, чтобы потенциальная угроза одному правозащитнику или организации была сама по себе менее эффективной

- Вы можете сделать выбор и **избежать** риска путем изменения или прекращения своей деятельности или путем изменения своей позиции во избежание потенциальных угроз.

- Вы можете **игнорировать** риск, не обращая на него внимания. Вряд ли стоит говорить о том, что это не лучший вариант.

Помните, что уровни риска обычно различны для каждой организации и отдельных лиц, вовлечённых в решение проблем, связанных с правами человека и что нападающие обычно наносят удар по самым слабым местам, поэтому вы должны делать скидку на эти разные уровни риска и принимать соответствующие меры. Например, давайте рассмотрим пример крестьянина, убитого солдатами частной армии землевладельца. В это дело могут быть вовлечены несколько организаций и отдельных лиц, таких как группа юристов из ближайшего крупного города, местный крестьянский профсоюз и три свидетеля (крестьяне, проживающие в соседней деревне). Чтобы правильно спланировать меры безопасности для каждого из них, здесь принципиально важно оценить различные уровни риска для всех участников событий.

Таблица 3: Информация, необходимая для оценки уязвимых мест группы и её и способностей к защите

(Примечание: В целом, информация в правой колонке может указывать на то, что каждый конкретный компонент левой колонки есть либо уязвимое место, либо способность данного правозащитника или данной группы правозащитников к защите).

КОМПОНЕНТЫ УЯЗВИМЫХ МЕСТ И РЕСУРСОВ	ІИНФОРМАЦИЯ, НЕОБХОДИМАЯ ДЛЯ ОЦЕНКИ УЯЗВИМЫХ МЕСТ ЛИБО РЕСУРСОВ НИЖЕПЕРЕЧИСЛЕННЫХ КОМПОНЕНТОВ
ГЕОГРАФИЧЕСКИЕ, ФИЗИЧЕСКИЕ И ТЕХНИЧЕСКИЕ КОМПОНЕНТЫ (СОСТАВЛЯЮЩИЕ)	
ОТКРЫТОСТЬ	Необходимость пребывания внутри опасной зоны либо прохода через неё для осуществления повседневной либо нерегуляной деятельности. Присутствие в этих зонах персонажей, представляющих угрозу.
ФИЗИЧЕСКИЕ СТРУКТУРЫ	Характеристики помещений (офисов, жилых зданий, укрытий), строительных материалов, дверей, окон, шкафов, защитных барьеров, ночного освещения.
ОФИСЫ И МЕСТА, ОТКРЫТЫЕ ДЛЯ ПУБЛИКИ	Открыты ли ваши офисы для посторонних лиц? Есть ли в них помещения, предназначенные сугубо для штатных сотрудников? Приходится ли вам иметь дело со случайными посетителями?
МЕСТА УКРЫТИЙ, МАРШРУТЫ ЭВАКУАЦИИ	Имеются ли у вас места укрытий? Насколько они доступны (физическое расстояние) и для кого (для отдельных лиц или для группы)? Можете ли вы на время покинуть зону в случае необходимости?
ДОСТУП В ЗОНУ	Насколько сложно для посторонних посетителей (правительственных чиновников, представителей НПО и т.д.) попасть в зону, например, в случае усли она находится в опасном регионе? Насколько ограничен доступ в неё для лиц, представляющих угрозу?
ТРАНСПОРТ И ЖИЛЬЕ	Имеют ли правозащитники доступ к безопасному транспорту (общественному или частному)? Имеет ли каждый из этих видов транспорта свои преимущества либо недостатки? Имеют ли правозащитники доступ к безопасному жилью во время командировок?
СВЯЗЬ	Установлены ли системы средств связи (радио, телефон)? Имеют ли правозащитники свободный доступ к ним? Работают ли средства связи нормально и непрерывно? Могут ли эти средства связи быть отрезаны носителями угроз в предверии нападения?

КОМПОНЕНТЫ УЯЗВИМЫХ МЕСТ И РЕСУРСОВ ЗАЩИТЫ	ИНФОРМАЦИЯ, НЕОБХОДИМАЯ ДЛЯ ОЦЕНКИ УЯЗВИМЫХ МЕСТ ЛИБО РЕСУРСОВ НИЖЕПЕРЕЧИСЛЕННЫХ КОМПОНЕНТОВ
КОМПОНЕНТЫ, СВЯЗАННЫЕ С КОНФЛИКТАМИ	
СВЯЗИ С КОНФЛИКТУЮЩИМИ СТОРОНАМИ	Имеют ли правозащитники связи с конфликтующими сторонами (являются ли они их родственниками, просходят ли из одного и того же региона, имеют ли схожие с ними интересы), которые могут быть использованы против них?
ДЕЙСТВИЯ ПРАВОЗАЩИТНИКОВ, ВЛИЯЮЩИЕ НА ОДНУ ИЗ КОНФЛИКТУЮЩИХ СТОРОН	Влияет ли деятельность правозащитников непосредственно на интересы одного из персонажей? (Например: при защите ценных природных ресурсов, прав собственности на землю либо прочих потенциальных интересов могущественных лиц.) Затрагивает ли ваша деятельность проблемы, к которым влиятельные персонажи (такие, например, как землевладельцы) особенно чувствительны?
ТРАНСПОРТИРОВКА ПРЕДМЕТОВ, ТОВАРОВ И ПЕЧАТНОЙ ИНФОРМАЦИИ	Располагают ли правозащитники предметами либо или товарами, которые могут представлять ценность для вооруженных групп и, в силу этого, усиливать риск нападения (бензин, предметы гуманитарной помощи, аккумуляторные батареи, руководства по правам человека и по оказанию медицинской помощи и т.д.)?
ИНФОРМАЦИЯ О БОЕВЫХ ДЕЙСТВИЯХ И ЗАМИНИРОВАННЫХ ЗОНАХ	Имеются ли у вас сведения о зонах боевых действий, которые могут представлять для вас риск? Либо о зонах безопасности? Есть ли у вас достоверная информация о заминированных районах?
КОМПОНЕНТЫ (СОСТАВЛЯЮЩИЕ), СВЯЗАННЫЕ С ЮРИДИЧЕСКОЙ И ПОЛИТИЧЕСКОЙ СИСТЕМОЙ	
ДОСТУП К ВЛАСТЯМ И К ЮРИДИЧЕСКОЙ СИСТЕМЕ ДЛЯ ЗАЩИТЫ ВАШИХ ПРАВ	Могут ли правозащитники инициировать юридические процессы для защиты своих прав? (Доступ к юридическому представительству, физическое присутствие на судебных процессах или консультациях и т.д.). Могут ли правозащитники получить необходимую помощь от соответствующих властей в соответствии с требованиями своей работы и безопасности? and protection needs?
СПОСОБНОСТЬ ДОБИТЬСЯ РЕЗУЛЬТАТОВ ОТ ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЫ И ОТ ОФИЦИАЛЬНЫХ ВЛАСТЕЙ	Имеют ли правозащитники юридическое право на защиту своих прав? Или же на них распространяется действие репрессивных внутригосударственных законов? Могут ли они добиться достаточного влияния, чтобы заставить власти обратить внимание на свои требования?
РЕГИСТРАЦИЯ, СПОСОБНОСТЬ ВЕСТИ БУХГАЛТЕРСКИЙ УЧЁТ И СОБЛЮДАТЬ ПРАВОВЫЕ НОРМЫ	Отказывают ли правозащитникам в юридической регистрации либо регистрация производится с большими задержками? Способна ли их организация надлежащим образом вести бухгалтерский учёт и соблюдать правовые нормы страны? Пользуетесь ли вы «пиратскими» компьютерными программами?
УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ	
ИСТОЧНИКИ И ДОСТОВЕРНОСТЬ ИНФОРМАЦИИ	Имеют ли правозащитники надежные источники информации для своих обвинений? Обнародывают ли правозащитники информацию с достаточной степенью достоверности и в достаточной ли мере?
ХРАНЕНИЕ, ОТПРАВКА И ПОЛУЧЕНИЕ ИНФОРМАЦИИ	В состоянии ли правозащитники хранить информацию в безопасном и надежном месте? Можно ли ее выкрасть? Возможно ли защитить её от вирусов и хакеров? Можете ли вы безопасно отправлять и получать информацию?
СВИДЕТЕЛЬСКИЕ ПОКАЗАНИЯ И ЛИБО ОБЛАДАНИЕ КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ	Являются ли правозащитники главными свидетелями при выдвижении обвинений против какого-либо могущественного персонажа? Обладают ли они уникальной информацией, имеющей отношение к данному судебному делу либо процессу?
НАЛИЧИЕ ЛОГИЧЕСКИ ОБОСНОВАННОГО И ПРИЕМЛЕМОГО ОБЪЯСНЕНИЯ ВАШЕЙ РАБОТЫ И ЕЁ ЦЕЛЕЙ	Имеют ли правозащитники четкое, веское и логически обоснованное объяснение своей работы и её целей? Является ли это объяснение приемлемым или хотя бы допустимым для большинства/всех участников событий (особенно для вооруженных)? В состоянии ли все члены группы предоставить такое объяснение в случае необходимости?

КОМПОНЕНТЫ УЯЗВИМЫХ МЕСТ И РЕСУРСОВ ЗАЩИТЫ	ИНФОРМАЦИЯ, НЕОБХОДИМАЯ ДЛЯ ОЦЕНКИ УЯЗВИМЫХ МЕСТ ЛИБО РЕСУРСОВ НИЖЕПЕРЕЧИСЛЕННЫХ КОМПОНЕНТОВ
СОЦИАЛЬНЫЕ И ОРГАНИЗАЦИОННЫЕ КОМПОНЕНТЫ (СОСТАВЛЯЮЩИЕ)	
НАЛИЧИЕ ОРГАНИЗАЦИОННОЙ СТРУКТУРЫ ГРУППЫ	Имеет ли группа какую-либо организацию? Обеспечивает ли эта организационная структура приемлемый уровень сплочённости группы?
СПОСОБНОСТЬ ПРИНИМАТЬ СОВМЕСТНЫЕ РЕШЕНИЯ	Отражает ли структура группы специфические интересы или представляет всю группу (в совокупности)? Осуществляется ли исполнение основных обязанностей и принятие решений одним либо несколькими людьми? Действуют ли системы дублирования для принятия решений и распределения обязанностей? В какой степени принятие решений является коллегиальным? Обеспечивает ли структура группы: а) коллегиальное принятие решений и их выполнение, б) коллегиальное обсуждение проблем, в) проведение спорадических и неэффективных дискуссий, г) не отвечает ни одному из вышеперечисленных пунктов?
ПЛАНЫ И МЕРЫ БЕЗОПАСНОСТИ	Задействованы ли правила и меры безопасности? Существует ли широкое понимание необходимости обладания соблюд средствами безопасности и их функций? Соблюдают ли сотрудники правила безопасности? (Дополнительная информация в Главе 8).
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В НЕРАБОЧЕЕ ВРЕМЯ (СЕМЬЯ И ДОСУГ)	Как правозащитники проводят свой досуг? Пьянство и принятие наркотиков представляют собой серьёзные факторы уязвимости. Внутрисемейные отношения – в зависимости от их характера - также способны привести как к повышению общей уязвимости, так и к её снижению.
УСЛОВИЯ РАБОТЫ	Со всеми ли заключены соответствующие рабочие контракты? Доступны ли резервные фонды и страховые полисы?
НАЕМ РАБОТНИКОВ	Есть ли у вас отлаженные процедуры приема на работу постоянных либо временных сотрудников либо членов группы? Есть ли у вас свой особые правила безопасности для волонтеров (например, студентов) или посетителей,?
РАБОТА С ЛЮДЬМИ ЛИБО С ОРГАНИЗАЦЯМИ -ПАРТНЕРАМИ	Работаете ли вы непосредственно с людьми? Хорошо ли вы знаете этих людей? Взаимодействуете ли вы с какой-либо организацией в качестве связующего звена в вашей работе с людьми?
ЗАБОТА О СВИДЕТЕЛЯХ ЛИБО ПОСТРАДАВШИХ	Оцениваем ли мы риск для пострадавших, свидетелей и т.д. при решении конкретных проблем? Есть ли у нас специальные меры безопасности для встреч с ними либо для их посещений офиса? Если им угрожают, каковы наши действия?
ОСОБЕННОСТИ РЕГИОНА И СОЦИАЛЬНАЯ СРЕДА	Хорошо ли правозащитники социально интегрированы в регионах? Рассматривают ли некоторые социальные группы работу правозащитников как полезную или , напротив, как приносящую вред? Окружены ли правозащитники потенциально враждебными людьми (к примеру, соседями-осведомителями)?
СПОСОБНОСТЬ К МОБИЛИЗАЦИИ	Способны ли правозащитники мобилизовать людей на публичные действия?

КОМПОНЕНТЫ УЯЗВИМЫХ МЕСТ И РЕСУРСОВ К ЗАЩИТЫ	ИНФОРМАЦИЯ, НЕОБХОДИМАЯ ДЛЯ ОЦЕНКИ УЯЗВИМЫХ МЕСТ ЛИБО РЕСУРСОВ ЗАЩИТЫ НИЖЕПЕРЕЧИСЛЕННЫХ КОМПОНЕНТОВ
ПСИХОЛОГИЧЕСКИЕ КОМПОНЕНТЫ (ГРУППА/ОТДЕЛЬНЫЕ ЛИЦА)	
СПОСОБНОСТЬ КОНТРОЛИРОВАТЬ СТРЕСС И СТРАХ	Уверены ли ключевые фигуры или вся группа в целом в своей работе? Открыто ли они выражают чувство единства и общей цели (на словах и в поступках)? Нарушается ли взаимодействие и межличностные отношения в результате повышенного уровня стресса?
ГЛУБОКИЙ ПЕССИМИЗМ ЛИБО БОЯЗНЬ ПРЕСЛЕДОВАНИЯ	Проявляются ли (в словах и в поступках) депрессия и безнадежность?
РАБОЧИЕ РЕСУРСЫ	
СПОСОБНОСТЬ ОСОЗНАВАТЬ КОНТЕКСТ РАБОТЫ И РИСК	Имеют ли правозащитники доступ к точной информации об условиях их работы, других участниках событий и их интересах? Способны ли правозащитники проанализировать эту информацию и осознать угрозы, уязвимые места и ресурсы защиты?
СПОСОБНОСТЬ ОПРЕДЕЛЯТЬ ПЛАН Ы ДЕЙСТВИЙ	Могут ли правозащитники определить, а, главное, осуществить планы действий? Можно ли привести соответствующие примеры из прошлого?
СПОСОБНОСТЬ ПОЛУЧИТЬ СОВЕТ ИЗ ХОРОШО ОСВЕДОМЛЕННЫХ ИСТОЧНИКОВ	Может ли группа получить надежный совет? Из надежных источников? Может ли группа сделать собственный выбор в вопросе, какой источник информации ей использовать? Есть ли у вас доступ к каким-либо специальным организациям или статус членства в них, способный повысить эффективность вашей защиты?
ЛЮДИ И ОБЪЕМ РАБОТЫ	Достаточно ли имеющихся в вашем распоряжении людей либо сотрудников для выполнения запланированного объема работы? Можете ли вы планировать групповые (не менее двух человек) выезды на места событий?
ФИНАНСОВЫЕ РЕСУРСЫ	Достаточно ли у вас финансовых ресурсов для вашей безопасности? Можете ли вы свободно распоряжаться наличными деньгами?
ЗНАНИЕ ЯЗЫКОВ И РЕГИОНА	Знаете ли вы языки, необходимые для работы в этом регионе? Хорошо ли вы знаете этот регион (дороги, населенные пункты, общественные телефоны, больницы и т.д.)?
ДОСТУП К НАЦИОНАЛЬНЫМ И МЕЖДУНАРОДНЫМ ПРЕДСТАВИТЕЛЬСТВАМ И СРЕДСТВАМ МАССОВОЙ ИНФОРМАЦИИ	
ДОСТУП К НАЦИОНАЛЬНЫМ И МЕЖДУНАРОДНЫМ ОРГАНИЗАЦИЯМ	Имеют ли правозащитники доступ к национальным и международным представительствам? К их делегациям, прибывающим с визитами, к посольствам, правительствам иных стран и т.д.? К лидерам общин, религиозным лидерам и к прочим влиятельным лицам? Можете ли вы организовать срочные акции через посредство других групп?
РЕЗУЛЬТАТИВНЫЙ ДОСТУП К СРЕДСТВАМ МАССОВОЙ ИНФОРМАЦИИ	Имеют ли правозащитники доступ к средствам массовой информации (национальным и международным)? К другим (в том числе, независимым) средствам массовой информации? Знают ли правозащитники как правильно строить отношения со средствами массовой информации?

Весы риска: ещё один способ его распознания

Весы представляют собой ещё один способ осознания настоящей концепции риска: На рисунке перед вами – так называемый «счётчик риска». Если мы поставим на одну чашу весов две коробки - с угрозами нам и с нашими уязвимыми местами, а на другую - одну коробку с нашими ресурсами защиты, то увидим, как повышается или снижается наш риск.

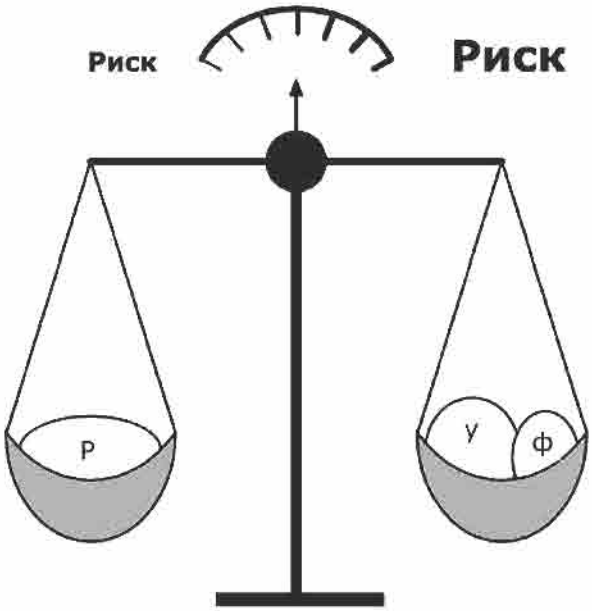


Рис. 1.

Чем больше угроз и факторов уязвимости, тем больше риск, с которым мы сталкиваемся:

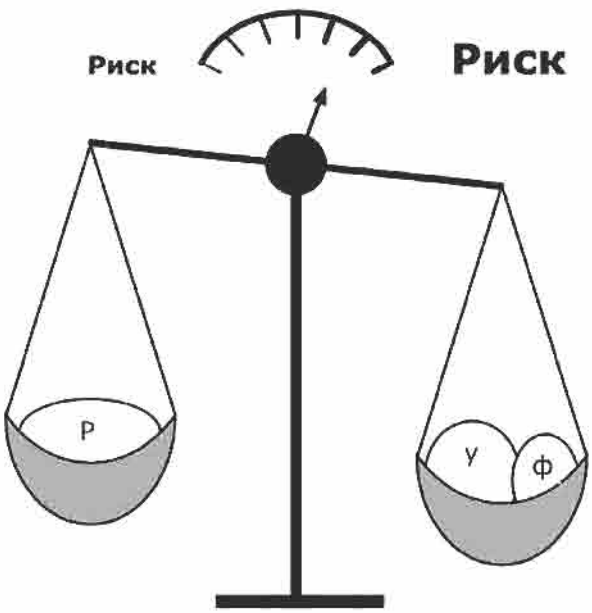


Рис. 2

Чем больше наши ресурсы (способности к защите), тем меньше наш риск. Чтобы снизить риск мы можем снизить уровень угрозы и сократить число факторов уязвимости, либо увеличить наши защитные ресурсы.

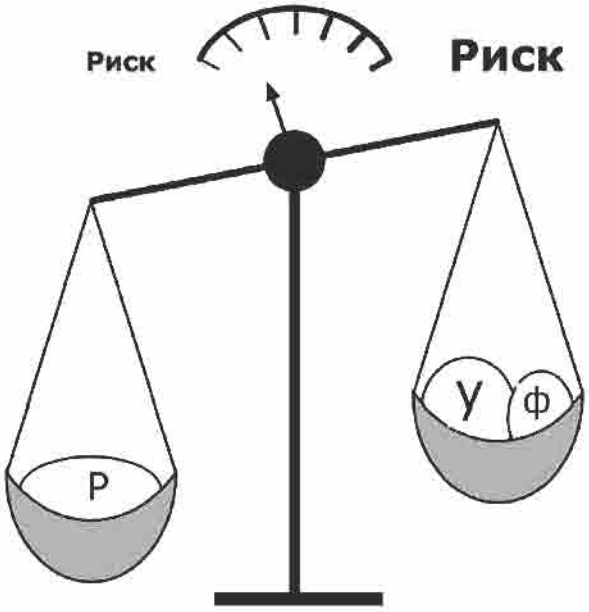


Рис. 3.

Но ... посмотрите, что произойдет, если мы столкнёмся с по-настоящему серьёзными угрозами: как бы мы не пытались усилить наши ресурсы в этот момент, весы все равно покажут высокий уровень риска!

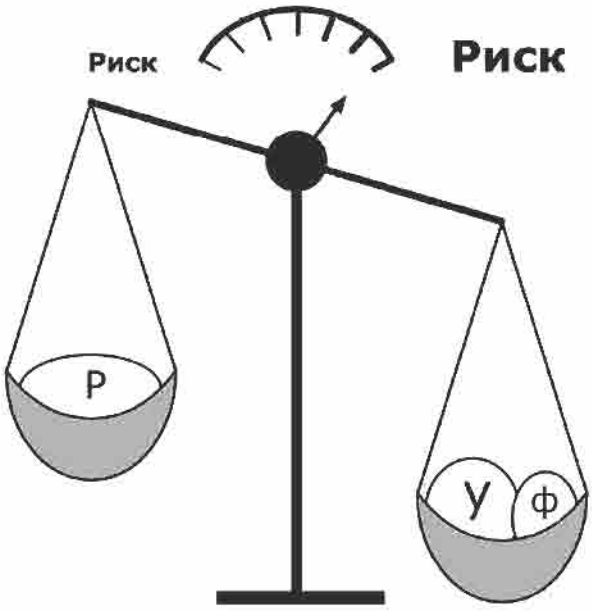


Рис. 4.

ОСОЗНАНИЕ И ОЦЕНКА УГРОЗ

Цель

Глубокое осознание угроз и способы реагирования на них.

Оценка угроз: Глубокое осознание угроз

Давление на правозащитников носит сугубо психологический характер. Угрозы широко применяются, чтобы заставить правозащитников почувствовать свою уязвимость, вызвать у них чувство беспокойства, смятения и беспомощности. Конечная цель подобных репрессий - внести раскол в эти организации и заставить правозащитников потерять веру в своих лидеров и коллег. Правозащитникам приходится балансировать между осторожной и адекватной реакцией на угрозы и сохранением ощущения того, что их работа продолжает оставаться безопасной. Этой теме и посвящена настоящая глава.

В Главе 2 угрозы определялись как «возможность того, что кто-то причинит физический или моральный ущерб личности либо имуществу путем умышленного и зачастую насильственного действия».

Мы также говорили о **возможных** угрозах (когда угрожают правозащитнику, имеющему близкое отношение к вашей работе, и есть основания считать, что вы можете стать следующим объектом угроз), а также о **реальных** угрозах (например, угроза убийства). Давайте сейчас рассмотрим, как реагировать на реальные угрозы.

Реальная угроза – это **декларация намерения нанести ущерб, наказать или причинить боль, обычно с целью достижения чего-либо, либо намёк на подобное намерение.** Правозащитники получают угрозы в связи со своей работой, и большинство угроз направлены либо на прекращение их деятельности, либо на то, что бы направить её в иное русло.

Угроза всегда имеет **источник**, т.е. лицо либо группа лиц, интересы которых задеты деятельностью правозащитника. Угроза также имеет **цель**, которая связана с результатами деятельности правозащитника, а также **средства выражения**, т.е. способ, с помощью которого она доводится до его сведения.

Угрозы, как правило, неоднозначны. С определенной степенью иронии можно утверждать, что они в какой-то мере «экологичны», поскольку нацелены на достижение максимальных результатов при минимальных затратах энергии. Человек, формулирующий угрозу, сделал именно такой выбор и предпочел его действиям, требующим большего вклада энергии. Почему? Ниже приводится ряд возможных причин:

- Лицо, формулирующее угрозу, имеет возможность действовать, но в определенной мере озабочено политическими издержками открытых акций против правозащитника. По этой же причине, могут возникать анонимные угрозы.

- Лицо, формулирующее угрозу, имеет ограниченную возможность действия и стремится скрыть это, подменяя её угрозой действия, на которые оно неспособно. Эта ограниченная способность к действию может иметь лишь временный (в связи с наличием иных приоритетов), либо постоянный характер, но в обоих случаях обстоятельства могут измениться и затем привести к прямым действиям против правозащитника.

Угроза есть насилие над личностью и потому она никогда не проходит бесследно. Иными словами, она так или иначе оказывает воздействие на людей. Один правозащитник как-то заметил: "Угрозы достигают определенного эффекта уже в силу того, что мы о них говорим". На практике любая угроза может обладать двойным действием: в эмоциональном плане и в плане безопасности. Мы затронем здесь лишь последний план, но не следует забывать и об эмоциональной стороне каждой угрозы.

Мы знаем, что угроза всегда связана с результатами нашей работы. Таким образом, получение угрозы представляет своеобразный «отклик» на то, в какой степени ваша деятельность повлияла на чьи-либо интересы. Исходя из этого, угроза является неоценимым источником информации и заслуживает пристального анализа.

Разница между формулированием угрозы и реальной опасностью

Люди угрожают правозащитникам по многим причинам, но только некоторые из них имеют намерение или возможность совершить акт насилия. В то же время, отдельные лица могут представлять серьезную угрозу, не выражая её на словах. Это отличие между формулированием угрозы и реальной опасностью её осуществления является весьма важным:

- Некоторые лица, изначально лишь **формулирующие** угрозу, впоследствие **становятся** её носителями.
- Многие **выразители** угроз сами по себе не представляют угрозы.
- Некоторые **никогда не выражающие** угроз лица на самом деле **представляют** угрозу.

Угроза достоверна лишь в том случае, когда она предполагает, что стоящий за ней человек способен предпринять направленные против вас действия. Она призвана заключать в себе некоторый уровень насилия либо провоцировать чувство страха.

Лицо, стоящее за угрозой, может легко продемонстрировать свою способность к её исполнению: например, подбросить угрожающую записку в закрытый салон автомобиля, даже если вы припарковали его всего на несколько минут, или позвонить вам сразу после того, как вы вернулись домой, тем самым давая понять, что за вами следят.

Люди могут попытаться вселить в вас страх путем выражения угрозы с помощью символов: например, направить вам приглашение на ваши собственные похороны либо подбросить на крыльцо вашего дома или в вашу постель труп какого-нибудь животного.

Многие угрозы представляют собой сочетание вышеуказанных элементов. Между ними важно проводить различие, так как некоторые выразители угроз, используя символы и запугивание, лишь делают вид, что они способны к реальным действиям.

Угрожать могут все, но не все представляют реальную угрозу.

В конечном итоге, вам необходимо знать, может ли угроза быть приведена в исполнение. Если вы обоснованно уверены, что это маловероятно, то вы будете действовать совсем не так, как в случае реальной угрозы.

Две основные задачи при оценке угрозы заключаются в следующем:

- Получить как можно больше информации о цели и источнике угрозы (и то и другое будет связано с вашей деятельностью).

- Прийти к логическому заключению о том, будет ли угроза реализована либо нет.

Пять этапов оценки угрозы

1• **Установить факты, сопровождавшие угрозу(-ы).** Важно точно уяснить, что произошло. Это можно сделать путем бесед либо опроса ключевых фигур, а иногда – с помощью анализа имеющейся информации.

2• **Установить, использовалась ли подобная система угроз в прошлом.** В случае многократных угроз (как это часто бывает) важно определить наличие в них сходных элементов, таких как способы и время их формулирования, символика, форма подачи (письменно либо устно) и т.д. Установить такие закономерности не всегда представляется возможным, но они важны для правильной оценки угрозы.

3• **Установить цель угрозы.** Поскольку угроза обычно имеет очевидную цель, связанную с результатами вашей деятельности, анализ этих результатов может помочь вам установить, какие цели преследует угроза.

4• **Установить, от кого исходит угроза.** (Это можно сделать только после завершения первых трех этапов). Постарайтесь быть как можно более конкретным. Например, вы можете заключить, что вам угрожает "правительство". Но, поскольку любое правительство представляет собой совокупность персонажей, то было бы полезнее установить, какие правительственные департаменты могут стоять за этими угрозами. Такие персонажи как «силы безопасности» и «партизанские формирования» также представляют собой совокупность персонажей. Помните, что даже подписанная угроза может быть сфабрикованной, что может быть удобно для выразителя, стремящегося избежать политических издержек и, тем не менее, достичь своей цели и приостановить деятельность правозащитника путем его запугивания.

5• **Сделать обоснованное заключение о том, может ли угроза быть приведена в исполнение.** Насилие условно. Вы никогда не можете быть полностью уверены в том, будет ли угроза приведена в исполнение либо нет. Прогнозирование возможности насилия сводится к констатации того, что при определенных обстоятельствах есть очевидный риск того, что какое-то конкретное лицо либо группа лиц способны применить насилие в отношении выбранной ими жертвы.

Правозащитники – не пророки и не в состоянии предсказывать будущее. Тем не менее, вы можете прийти к обоснованному заключению о вероятности либо маловероятности приведения в исполнение той или иной угрозы. Завершив первые четыре этапа оценки, вы, возможно, ещё не получите достаточной информации об угрозе и, следовательно, не сможете прийти к какому-либо заключению. У вас также могут быть различные мнения относительно того, насколько «реальна» данная угроза. В любом случае, ваши действия должны всегда быть основаны на ожидании худшего.

Например:

> Правозащитник получил угрозы убийства. Группа проводит анализ угроз и делает два противоположных вывода, причем оба основаны на убедительной аргументации. Некоторые члены группы утверждают, что угрозы – абсолютный блеф, а другие усматривают в этих угрозах тревожные признаки их реальности. В конце обсуждения, группа решает исходить из наихудшегос ценария: что угроза реальна - и принимает соответствующие меры безопасности.

Оценка угрозы прогрессирует от твердых фактов (шаг 1) до усиливающегося спекулятивного рассуждения. Второй шаг (шаг 2) вовлекает некоторую интерпретацию фактов и увеличивается далее через шаги три, четыре, пять. Для следования этого порядка шагов имеются серьезные основания. Для примера, если вы следуйте прямо к действиям шагов 2 или 4, то вы упускаете основательную информацию вытекающую из предыдущих шагов.

Поддержание и снятие фактора угрозы

Угроза либо инцидент, связанный с безопасностью, в состоянии встревожить правозащитников, но оставаться настороже до самого исчезновения угрозы обычно бывает трудно. В связи с постоянным давлением извне, оказываемым на правозащитников в процессе их работы, слишком частые сигналы тревоги могут привести к тому, что группа утратит к этому интерес и ослабит бдительность.

Поднимать тревогу в группе следует лишь на основании достоверных фактов и по поводу конкретного ожидаемого события. Подобная тревога призвана нацелить членов группы на специфические дествия. Для достижения максимальной эффективности, сигнал тревоги должен стимулировать лишь умеренный уровень мотивации: слишком низкий уровень не побуждает людей к действию, а слишком высокий - создает эмоциональные перегрузки. Если есть вероятность того, что угроза будет длительной, то необходимо опросить задействованных лиц дважды – сразу же после получения сигнала и некоторое время спустя – с целью корректировки информации и рекомендаций, а также для укрепления веры участников группы в их совместные усилия.

И, наконец, если угроза не была осуществлена, необходимо объяснить причину этого и уведомить группу о том, что угроза уменьшилась или полностью исчезла.

Вы можете ставить вопрос о снятии фактора угрозы только после установления того, что источник её более не опасен. В идеале, прежде чем убедиться в правомерности снятия угрозы, вы должны быть в состоянии объяснить, почему вы это делаете. Следует также принять во внимание возможное изменение обстоятельств, которые смогут подтолкнуть человека, стоящего за угрозами, к насильственным действиям.

Реакция на угрозы с позиции безопасности

- Угроза может рассматриваться как инцидент, связанный с нарушением безопасности. Для получения более подробной информации о реагировании на подобные инциденты см. Главу 4.

- Анализ объявленных угроз может привести вас к мысли о том, что на вас может быть совершено нападение. О том, как предотвратить такое нападение, читайте в Главе 5.

Глава 4

Инциденты, связанные с безопасностью: определение и анализ

Цель

Как распознать инциденты, связанные с нарушением безопасности, и как реагировать на них

Что такое инцидент, связанный с безопасностью?

Попросту говоря, инцидент, связанный с безопасностью (либо с её нарушением) можно определить как **любой факт или событие, которое, по вашему мнению, может повлиять на вашу личную безопасность или безопасность вашей организации.**

К примерам подобных инцидентов можно отнести неоднократно замеченный подозрительный автомобиль, припаркованный в течение нескольких дней возле вашего офиса или дома, телефонные звонки в ночное время с молчанием на другом конце провода, расспросы о вас среди жителей ближайшего города или деревни, вторжение в ваш дом и т.д.

Но не всё, на что вы обращаете внимание, представляет собой инцидент, связанный с безопасностью. Поэтому вы должны **регистрировать** подобные случаи и впоследствии **анализировать** их, желательно вместе с коллегами, чтобы установить в состоянии ли они повлиять на вашу безопасность. После этого, вы можете **реагировать** на инциденты в следующей последовательности:

> Вы что-то замечаете ⇨ вы осознаете, что это может быть инцидент, связанный безопасностью ⇨ вы регистрируете его/сообщаете о нем коллегам ⇨ анализируете его ⇨ устанавливаете, что это инцидент, связанный с безопасностью ⇨ реагируете на него соответствующим образом.

Даже если вопрос требует срочного внимания, все равно следует соблюдать вышеобозначенную последовательность действий, но гораздо быстрее, чем обычно. (см. ниже).

Как отличить инциденты, связанные с безопасностью, от угроз:

Если вы ожидаете автобус и кто-нибудь, стоящий рядом, угрожает вам в связи с вашей работой, то это не только угроза, но ещё и инцидент, связанный с безопасностью. Но если вы обнаружите, что за вашим офисом ведется наблюдение из полицейской машины с противоположной стороны улицы, либо что украден ваш мобильный телефон – то это инциденты, связанные с безопасностью, но не обязательно угрозы. Помните: угрозы имеют некую цель (см. Главу 2), а инциденты просто случаются.

Все угрозы представляют собой инциденты, связанные с безопасностью,
но не все инциденты, связанные с безопасностью, являются угрозами.

Почему так важны инциденты, связанные с безопасностью?

Инциденты, связанные с безопасностью, принципиально важны для вашей защиты, так как о**ни дают важнейшую информацию о результатах вашей работы и о возможных акциях, планируемых или проводимых против вас.** Кроме того, такие инциденты позволяют вам изменить ваше поведение или деятельность, а также избегать опасных мест. Таким образом, инциденты, связанные с безопасностью, могут рассматриваться как показатели состояния локальной защиты. Если бы вам не удалось учесть этих показателей, то принятие своевременных и адекватных мер для обеспечения вашей безопасности будет затруднительным.

Например, после того как вы обратили внимание на несколько инцидентов, связанных с безопасностью, вы могли понять, что за вами следят и принять соответсствующие меры.

Инциденты, связанные с безопасностью, представляют собой «минимальную единицу» измерения защиты и свидетельствуют о наличии сопротивления вашей рабете либо о давлении на неё.
Не оставляйте их без внимания!

Когда и как вы заметили инциденты, связанные с безопасностью?

Это зависит от того, насколько очевиден инцидент. Если бы он потенциально мог пройти незамеченным, то ваша способность к его распознанию зависит от вашей подготовки в вопросах безопасности, опыта и уровня осведомленности.

Чем выше ваша осведомленность и чем тщательней подготовка, тем меньше инцидентов пройдет мимо вашего внимания.

Иногда инциденты, связанные с безопасностью, проходят незамеченными либо едва замеченными и поэтому игнорируются. В иных случаях наблюдается чрезмерная реакция на предполагаемый инцидент, связанный с безопасностью.

Почему инцидент, связанный с безопасностью может пройти незамеченным?

Пример:

Правозащитник становится объектом инцидента, связанного с безопасностью, но организация, в которой он/она работает, совершенно на это не реагирует. Такое может происходить потому, что...

- правозащитник не осознает, что произошел инцидент, связанный с его безопасностью.
- правозащитник осознает инцидент, но не обращает на него внимания.
- правозащитник не уведомил организацию (он/она забыл это сделать, посчитал, что в этом нет необходимости или решил скрыть этот факт, полагая, что это произошло из-за его/её ошибки).
- организация, в результате коллегиальной оценки инцидента после его регистрации в журнале инцидентов, считает, что оснований для принятия мер нет.

Почему люди иногда чрезмерно реагируют на инциденты, связанные с безопасностью?

Пример:

Возможно, кто-либо из коллег постоянно рассказывает истории о каких-то инцидентах, связанных с безопасностью, но при более внимательном анализе оказывается, что они таковыми не являются . В этом случае реальный инцидент, связанный с безопасностью, состоит в том, что ваш/а коллега воображает несуществующие инциденты. Он/она, возможно, испытывает сильное чувство страха либо страдает от стресса и нуждается в поддержке для решения этой проблемы.

Не забывайте, что слишком часто инциденты, связанные с безопасностью, проходят незамеченными или их не воспринимают всерьез: Будьте внимательны!

Реакция на инциденты, связанные с безопасностью

Проблемы инцидентов, связанных с безопасностью, можно решить с помощью трех основных процедур:

1 • **Зарегистрировать их.** Любой инцидент, связанный с безопасностью и замеченный правозащитником, должен быть зарегистрирован в его/её личной записной книжке либо в книге записей, доступной для всей группы.

2 • **Проанализировать их.** Все зарегистрированные инциденты, связанные с безопасностью, должны тотчас же (либо регулярно) анализироваться. Их лучше анализировать группой, а не в одиночку, так как это снижает риск того, что что-то будет упущено. Кто-то должен руководить этим процессом для доведения его до конца.

Необходимо также принять решение о том сохранять или не сохранять конфиденциальность в отношении тех или иных инцидентов, связанных с безопасностью (таких как угрозы). Этично ли и реально ли скрыть угрозу от коллег и других людей, с которыми вы работаете? Здесь, конечно, возможны исключения, но часто лучше быть максимально открытым в подаче информации и вразрешении тактических вопросов (в том числе и причин чувства страха и беспокойства среди коллег).

3 • **Отреагировать на них.** Учитывая, что инциденты, связанные с безопасностью, являются своеобразным «отзывом» (либо «откликом») на вашу работу, они могут привести к следующему:

- Реакции на сам инцидент
- **«Отзыв»** с позиции безопасности (защиты), о том как вы работаете, каковы ваши рабочие **планы** или **стратегия**.

Пример:

оинцидента, вызвавшего «отклик» на премет того, как вы планируете вашу защиту

У того же полицейского КПП вас задерживают на полчаса, говорят, что с неодобрением относятся к вашей работе и высказывают в ваш адрес едва прикрытые угрозы. Когдавы обращаетесь за разъяснениями в полицейское управление, то сцена повторяется. Тогда вы созываете свою группу для пересмотра планов работы, так как становится очевидным, что они нуждаются в корректировке. Далее вы планируете ряд встречс представителями Министерства внутренних дел, вносите изменения в некоторыеаспекты ваших планов и прово ите еженедельные совещания для контроля ситуации.

Пример:

оинцидента, вызвавшего «отклик» на предмет вашей стратегии безопасности:

Вы начинаете работу в качестве правозащитника в новом регионе и сразу же получаете угрозу убийства, а один из ваших коллег подвергается избиению. Вы не предполагали, что ваша работа вызовет такое противодействие и не приняли это во внимкние при разработке общей стратегии. Следовательно, для того, чтобы выработать терпимость к вашей работе в данном регионе и избежать дальнейших нападений и угроз, вам, скорее всего, придется изменить стратегию. Для этого, вы должны на некоторое время приостановить работу,выехать за пределы региона и пересмотреть весь проект.

Пример:

Быстрая реакция на инцидент, связанный с безопасностью:

Существует много способов быстрого реагирования на инциденты, связанные с безопасностью. Мы определили следующую последовательность действий по реагированию на инцидент с момента, когда о нем становится известно, в процессе его развития и после его завершения.

Быстрая реакция на инцидент, связанный с безопасностью

Существует много способов быстрого реагирования на инциденты, связанные с безопасностью. Мы определили следующую последовательность действий по реагированию на инцидент с момента, когда о нем становится известно, в процессе его развития и после его завершения.

1. Сообщите об инциденте коллегам.

- Что происходит/ произошло (постарайтесь сконцентрироваться на реальных фактах)?
- Где и когда он произошел?
- Кто к этому причастен (если это можно установить)?
- Привел ли он к телесным повреждениям либо к ущербу?

2. Примите решение о времени (моменте) реагирования. Здесь существует две возможности:

- **моментальная реакция** требуется в том случае, когда необходимо оказать помощь пострадавшим либо пресечь нападение в корне
- **быстрая реакция** (в течение нескольких часов или даже дней) необходима для предупреждения новых инцидентов, связанных с безопасностью.
- **последующая реакция** (в течение нескольких дней, недель или даже месяцев): если ситуация стабилизировалась, то в моментальной и быстрой реакции, возможно, нет необходимости. Тем не менее, любой инцидент, связанный с безопасностью, требующий немедленных или быстрых действий, должен сопровождаться принятием последующих мер с целью восстановления либо изменения условий вашей работы.

3. Примите решение о том, как именно реагировать и каковы ваши цели.

- Если требуется моментальная реакция, то в этом случае цели ясны: оказать помощь пострадавшим и/либо предупредить новые нападения.

- Если требуется быстрая реакция, то в этом случае цели определяются кризисной (или иной аналогичной) группой и **должны быть сфокусированы на восстановлении необходимой безопасности для потерпевших.**

Дальнейшие действия предпринимаются по отработанной в организации схеме принятия решений с целью восстановления безопасных внешних условий работы и внутренних организационных процедур, а также для совершенствования мер по реагированию на возможные инциденты, связанные с безопасностью, в будущем.

Любая реакция должна учитывать безопасность и защиту других лиц либо организаций и учреждений, с которыми вы имеете рабочие взаимоотношения.

Прежде чем действовать, определите ваши цели. Быстрое принятие мер важно, но ещё более важно знать, почему вы принимаете эти меры. Лишь установив, чего конкретно вы хотите достичь (цели), вы сможете принять решение о том, как достичь этого (порядок действий).

Например:

Если группа правозащитников узнаёт о том, что один из их коллег не прибыл в назначенное время в какой-либо город, она могут начать действовать с телефонных звонков в больницу, коллегам из других НПО либо в ближайшее представительство ООН или в полицию. Но, прежде чем звонить, очень важно определить, чего вы можете этим добиться и что вы собираетесь сказать. В противном случае, вы вызовете ненужную тревогу (представьте, что правозащитник задержался, потому что он опоздал на автобус и забыл позвонить в офис) или реакцию обратную той, на которую вы рассчитывали.

Предотвращение нападений и реакция на них

Цель

Оценка вероятности различных видов нападений.

Предотвращение возможных открытых нападений на правозащитников.
Принятие контр-мер против слежки.

Нападения на правозащитников

Насилие представляет собой одновременно процесс и действие. Насильственное нападение на правозащитника происходит не в вакууме. Тщательный анализ актов агрессии часто показывает, что они являются кульминацией конфликтов, споров, угроз и ошибок, имевших место на протяжение какого-то времени.

Нападения на правозащитников представляют собой результат по меньшей мере, трёх следующих взаимосвязанных факторов.

1 • **Субъекта насилия.** Нападения на правозащитников часто представляют собой результат объяснимых процессов мышления и поведения, из которых мы можем извлечь уроки, даже если они и являются противозаконными.

2 • **Подоплеки и катализаторов, побудивших нападающего сознательно прибегнуть к насилию.** Большинство людей, совершающих нападения на правозащитников, рассматривают его как способ достижения цели либо решения личной проблемы.

3 • **Обстановки** которая облегчает насилие, позволяет его совершить либо не препятствует ему.

Кто же опасен для правозащитников?

В принципе, любой, кто считает, что нападение на правозащитника является желательным, приемлемым либо потенциально эффективным способом достижения цели, может рассматриваться как возможный агрессор. Угроза усиливается, если он/она имеет или может прибрести ресурсы для такого нападения.

Некоторые нападения предваряются угрозами, а некоторые нет. Тем не менее, поведение людей, планирующих направленное насилие, часто является в некоторой стерени предсказуемым, поскольку им необходимо собрать информацию о времени, удобном для нападения, а также запланировать выход на цель и пути к отступлению после атаки.

Угроза нападения может снизиться с изменением ресурсов для него у потенциального агрессора, А также - его отношения к тому, насколько приемлемо такое нападение, и насколько велика вероятность того, что он/она будут пойманы и наказаны.

Поэтому принципиально важно подметить и проанализировать любые признаки, свидетельствующие о возможном нападении. Этот процесс включает в себя следующее:

- определение вероятности приведения угрозы в действие (см. Главу 3).
- определение и анализ инцидентов, связанных с безопасностью.

Инциденты, включающие слежку за правозащитниками или местом их работы, нацелены на сбор информации. Эта информация не всегда предназначена для осуществления самого нападения, и поэтому важно установить является ли она таковой или нет (см. Главу 4).

Наблюдение за персоналом либо офисом служит для сбора информации о них и может производиться с несколькими целями:

- Установить чем именно, а также когда и с кем, занимаются данные правозащитники.
- Использовать эту информацию позже для нанесения удара по отдельным лицам либо организациям.
- Собрать информацию, необходимую для осуществления нападения.
- Собрать информацию для подачи судебного иска либо иных преследований (без прямого насилия).
- Запугать ваших помощников либо других людей, работающих с вами, или предоставить в ваше распоряжение такую информацию, которая побудит вас прекратить сотрудничество с ними.

Важно помнить, что хотя предварительная слежка, как правило, необходима для осуществления нападения, сама по себе она не является актом агрессии. Более того, не всякая слежка непременно предшествует нападению. Преднамеренное нападение иногда происходит в ситуациях, когда нападающий внезапно видит возможность для нанесения удара, но даже тогда нападению, как правило, предшествует какая-то подготовка к нему.

Информация об успешном распознании признаков подготовки к нападению весьма скудна. Отсутствие исследований по этой теме резко контрастирует с огромным числом самих нападений на правозащитников. Тем не менее, уже имеющиеся в нашем распоряжении материалы позволяют сделать некоторые интересные обобщения[1].

1 Клаудиа Самайоа и Хосе Круз (Гватемала) и Хайме Прието (Колумбия) (Samayoa C., Cruz J. & Prieto J.) подготовили интересные исследования нападений правозащитников. Махони и Эгурен (Mahony and Eguren, 1997) также провели подобный анализ .

- **Нападение на правозащитника дело не простое и требует наличия определённых ресурсов.** Слежка необходима для установления маршрута передвижений того или иного лица и для выбора наиболее подходящего места для совершения нападения. Выход на цель и эффективное и быстрое отступление также очень важны. (Однако, если обстоятельства чрезвычайно благоприятны для нападающего, то это облегчает его задачу).

- **Лица, нападающие на правозащитников, как правило, руководствуются определенной степенью логики.** Большинство нападений нацелены на правозащитников, которые имеют самое непосредственное отношение к вопросам, затрагивающим интересы самих нападающих. Другими словами, нападения, как правило, осуществляются не наугад и не бесцельно; они отражают интересы тех, кто их совершает.

- **Географические факторы тоже имеют значение.** Например, нападения на правозащитников в сельской местности менее заметны для широкой публики и поэтому вызывают меньшую ответную реакцию у сил правопорядка и у политиков, чем нападения, совершенные в крупных городах. При этом, нападения на штаб-квартиры НПО или на известные организации в городах вызывают ещё большую реакцию.

- **Основные решения принимаются нападающими до нанесения удара.** Люди, готовящие нападение на организацию правозащитников, должны решить на кого совершить нападение:на лидеров или на рядовых членов, а также выбрать между единичным ударом, направленным на ключевую и ,возможно, высокопоставленную фигуру и, таким образом, понести более значительные политические издержки, либо на целом ряде ударов по нескольким членам правозащитной организации. Немногочисленные исследования нападений на правозащитников свидетельствуют о том, что, как правило, одновременно применяются обе стратегии.

Определение вероятности нападения

Для того, чтобы установить степень вероятности нападения, необходимо проанализировать соответствующие факторы. А для того, чтобы определить, в чём состоят эти факторы, целесообразно разграничить друг от друга различные виды нападения: обычные преступления, непреднамеренные нападения (появление не в том месте и не в то время) и прямые (целенаправленные) атаки - применяя три таблицы, приведенные ниже (Табл. 1, 2; с. 44-45)[2].

2 Такая классификация нападений включает те же категории что и угрозы: для уточнений см. главу об угрозах.

Таблица 1: Определение уровня угрозы прямого (целенаправленного) нападения

(**ПП** означает «потенциальные преступники»)

УРОВЕНЬ УГРОЗЫ ПРЯМОГО (ЦЕЛЕНАПРАВЛЕННОГО) НАПАДЕНИЯ			
ФАКТОРЫ	НИЗКИЙ УРОВЕНЬ УГРОЗЫ	СРЕДНИЙ УРОВЕНЬ УГРОЗЫ	ВЫСОКИЙ УРОВЕНЬ УГРОЗЫ
СПОСОБНОСТЬ К НАПАДЕНИЮ	ПП имеют ограниченную возможность действий в районах, где вы работаете	ПП имеют оперативную возможность действий вблизи районов, где вы работаете	Зоны, в которых вы работаете, находятся под жёстким контролем ПН
ФИНАНСОВЫЕ МОТИВЫ	ПП не испытывают нужды в вашем имуществе либо финансах	ПП заинтересованы в вашем имуществе , деньгах и других формах финансовых поступлений (напр., от выкупов за похищения людей)	ПН остро нуждаются в имуществе и финансах
ПОЛИТИЧЕСКИЕ И ВОЕННЫЕ МОТИВЫ	Отсутствуют – ваша работа не имеет ничего общего с их целями	Частичны: ваша работа ограничивает их политические и военные цели	Ваша работа однозначно влияет на их цели, благоприятствует их противникам и т.д.
РЕГИСТРАЦИЯ ПРЕДЫДУЩИХ НАПАДЕНИЙ	Отсутствовали или случались редко	Периодически имели место	Наблюдались многочисленные случаи
ПОЗИЦИИ ЛИБО НАМЕРЕНИЯ	Сочувствие либо безразличие	Безразличие, периодические угрозы, частые предупреждения	Агрессивные намерения, с явными и действительными угрозами
СПОСОБНОСТЬ СИЛ БЕЗОПАСНОСТИ ПРЕДУПРЕДИТЬ НАПАДЕНИЕ	Реальная	Низкая	Отсутствует, либо силы безопасности сотрудничают с ПН
ВАШ УРОВЕНЬ ПОЛИТИЧЕСКОГО ВЛИЯНИЯ НА ПН	Хороший	От среднего до низкого	Ограниченный (зависит от обстоятельств) либо нулевой

Пример

уровня угрозы прямого (целенаправленного) нападения:

ПН контролируют районы, в которых вы работаете, но у них нет никаких финансовых мотивов для нападения на вас. Ваша работа лишь частично ограничивает их политические и военные цели, и в городе не было прецедентов совершения аналогичных нападений. Их отношение безразлично, и они явно не хотят привлекать к себе внимание всей страны или ставить себя под удар, совершив на вас нападение.

Уровень угрозы прямого нападения в этом сценарии считается низким или средним.

Таблица 2: Определение уровня опасности стать жертвой преступления

(**ПП** означает «потенциальные преступники»)

УРОВЕНЬ УГРОЗЫ ПРЕСТУПЛЕНИЯ			
ФАКТОРЫ	НИЗКИЙ УРОВЕНЬ УГРОЗЫ	СРЕДНИЙ УРОВЕНЬ УГРОЗЫ	ВЫСОКИЙ УРОВЕНЬ УГРОЗЫ
МОБИЛЬНОСТЬ И МЕСТОНА-ХОЖДЕНИЕ ПП	ПП, как правило, пребывают на своей территорииб отдалённой от зон деятельности НПО	ПП, как правило, проникают на чужую территорию в ночное время (или действуют вблизи зон деятельности НПО)	ПП действуют повсюду, днём и ночью
АГРЕССИВНОСТЬ ПП	ПП избегают конфронтации (в основном совершая преступления в местах, где нет зон деятельности НПО)	ПП совершают преступления на улицах (но не в учреждениях)	ПП открыто совершают ограбления на улицах, врываются в помещения для совершения преступлений
ОРУЖИЕ: ДОСТУП К НЕМУ ЛИБО ЕГО ПРИМЕНЕНИЕ	невооружены или используют нелетальное оружие	Холодное оружие, включая мачете	Огнестрельное оружие, иногда мощное
РАЗМЕР И ОРГАНИЗАЦИЯ	Действуют индивидуально или в парах	2-4 человека действуют сообща	Действуют группами
РЕАКЦИЯ ПОЛИЦИИ И СДЕРЖИВАНИЕ	Быстрая реакция, достаточная для сдерживания	Медленная реакция, небольшая вероятность поимки преступников на месте преступления	Полиция никак не реагирует на преступления
ПОДГОТОВКА И ПРОФЕСС -ИОНАЛИЗМ СИЛ ПРАВОПОРЯДКА	Хорошая профессиональная подготовка, при отсутствии материального обеспечения	Регулярная подготовка, низкая оплата, ограниченное материальное обеспечение	Полиции либо вообще нет, либо она коррумпирована (сотрудничает с преступниками)
ОБЩЕЕ СОСТОЯНИЕ БЕЗОПАСНОСТИ	Процветает беззаконие, но ситуация относительно спокойная	Отсутствие безопасности	Права не соблюдаются, царит абсолютная безнаказанность

Пример

Оценки уровня угрозы преступления:

В этом городе преступники действуют в различных районах парами или небольшими группам, иногда в дневное время. Они агрессивны и часто имеют при себе оружие. Полиция на них реагирует, но медленно и неэффективно, вследствие нехватки профессионализма и недостаточного материального обеспечения. Тем не менее, руководство полиции имеет хорошую дисциплину. Налицо отсутствие безопасности и, применительно к маргинальным районам города, угроза преступления имеет максимальный уровень при условии, что **все** вышеуказанные показатели имеют максимальную величину.

Вероятность преступного нападения в центре такого города находится между высоким и средним уровнем.

Таблица 3: Определение уровня угрозы непрямых (непреднамеренных) нападений

(**ПП** означает «потенциальные преступники»)

УРОВЕНЬ УГРОЗЫ НЕПРЯМОГО НАПАДЕНИЯ			
ФАКТОРЫ	НИЗКИЙ УРОВЕНЬ УГРОЗЫ	СРЕДНИЙ УРОВЕНЬ УГРОЗЫ	ВЫСОКИЙ УРОВЕНЬ УГРОЗЫ
ВАШЕ ЗНАНИЕ ЗОН КОНФЛИКТА	Хорошее	Относительное	Вы знаете очень мало о местонахождении зон боевых действий
РАССТОЯНИЕ ДО ЗОН КОНФЛИКТА	Ваша работа находится далеко от этих зон	Ваша работа находится недалеко от этих зон, и иногда вы посещаете их	Ваша работа проводится в зонах боевых действий
ПЕРЕМЕЩЕНИЕ ЗОН КОНФЛИКТА	Зоны конфликтов статичны или перемещаются медленно и определимо	Зоны конфликтов изменяются сравнительно часто	Зоны конфликтов изменяются постоянно и непредсказуемо
ВАШЕ ЗНАНИЕ РАСПОЛОЖЕНИЯ МИННЫХ ПОЛЕЙ	Вы обладаете достоверной информацией, или таких полей нет	Ваше знание о расположении минных полей относительно	У вас нет никаких сведений
РАССТОЯНИЕ МЕЖДУ МЕСТОМ ВАШЕЙ РАБОТЫ И МИННЫМИ ПОЛЯМИ	Место вашей работы находится далеко от заминированных районов , либо таковых не имеется	Место вашей работы находится близко к заминированным районам и иногда вы посещаете их	Место вашей работы находится в заминированном районе
ТАКТИКА БОЕВЫХ ДЕЙСТВИЙ И вооружения	Упорядочена	Упорядочена, с периодическим использованием артиллерии, засад и снайперов	Хаотична: применение бомбардировок, тяжелой артиллерии, террористических ибо ,бомбовых нападений

Пример

Оценки уровня угрозы непрямого (непреднамеренного) нападения:

Вы знакомы с зонами боевых действий в этом районе. Они изменяются медленно и поддаются определению. Место вашей работы находится вблизи зон боевых действий, и иногда вы посещаете эти районы либо находитесь в них. Вы находитесь вдали от заминированных зон. Применяемая тактика ведения боевых действий упорядочена, и поэтому, гражданские лица страдают не часто.

Работа в таких зонах сопряжена с низким уровнем риска непрямого (непреднамеренного) нападения.

Предотвращение возможного прямого нападения

Теперь вы знаете, что угроза может уменьшаться с изменением у потенциальных нападающих возможности нанести удар, их отношения к целесообразности нанесения удара и степени вероятности того, что он/она будут пойманы и наказаны.

Таким образом, для предупреждения нападения необходимо:

- Убедить потенциального нападающего или лицо, заявившее об угрозе, в том, что нападение повлечет за собой неприемлемые для него издержки и последствия;
- Сделать так, чтобы нападение стало менее осуществимым.

Этот вид предупреждения нападения аналогичен анализу, проведенному в Главе 2, в которой говорится, что риск зависит от уязвимых мест и ресурсов защиты. В этой же главе сказано, что для того чтобы защитить себя и снизить риск, вам необходимо принять меры против угрозы, снизить вашу уязвимость и расширить ресурсы.

Таблица 4: Предупреждение прямого нападения – различные результаты защиты

ПРЕДУПРЕЖДЕНИЕ ПРЯМОГО НАПАДЕНИЯ – РАЗЛИЧНЫЕ РЕЗУЛЬТАТЫ ЗАЩИТЫ	
1 **Изменение поведения преступника:** предотвращение атак с помощью увеличения возможных затрат на атаку. 2 **Изменение в соблюдении заинтересованными сторонами Декларации ООН о правозащитниках:**[3] отговорить преступников от атак из-за того, что более вероятно, что власти будут защищать правозащитников и следить за преступников.	→ **Контролирование и снижение угроз: (путем противостояния непосредственно источнику угрозы либо действиям, предпринятым источником угрозы)**
3 **Сокращение возможности осуществления нападения:** свести к минимуму появление защитника на публике, улучшить вашу рабочую обстановку, управлять страхом и стрессом, развивать систему безопасности, и т.д.	→ **Снижение уязвимости, расширение ресурсов**

3 См. Главу 1. Например, после того, как правозащитник подаст жалобу в ответ на угрозы, прокурор, полиция или какой-либо другой орган начнет расследование происшествия и это приведет к действиям против тех, кто угрожает правозащитнику. В любом случае, это может быть целью реакции по предотвращению нападения.

Когда угроза объявлена, и вы хотите снизить связанный с ней риск, важно принять меры – не просто против самой угрозы, но и по снижению своей **уязвимости** и расширению **ресурсов** защиты, наиболее тесно связанных с этой угрозой. В период сильного напряжения, когда вы хотите действовать как можно быстрее, вы часто принимаете меры по защите не тех уязвимых мест, что более всего подвержены угрозе, а тех , которые легче всего защитить.

Будьте осмотрительны: Если риск нападения велик (т.е. угроза велика и реальна и существует несколько уязвимых мест, а ресурсы весьма ограничены), принятие мер по снижению уязвимости или расширению ресурсов вряд ли имеет смысл, так как на это требуется время. Если риск нападения велик (прямое и жестокое нападение неизбежно), вы можете принять только три меры чтобы избежать его:

а • Оказать немедленное и эффективное противодействие угрозе, понимая, что вы можете достичь немедленного и конкретного результата, способного предотвратить нападение (обычно очень трудно быть уверенным в том, что результат будет немедленным и эффективным, так как на реакцию требуется время, а в таких ситуациях время доорого).

б • Свести вашу уязвимость до минимума, спрятавшись в зоне опасности либо покинув её.[4]

в • Обращение за вооруженной защитой, исходя из того, что она находится рядом (то есть может быть задействована немедленно), может сдержать потенциальных нападающих и не ставит правозащитника в ещё более опасное положение в скором или более отдаленном времени (на практике, это очень трудно осуществить!). Иногда, вследствие общенационального или международного давления, правительство предлагает правозащитникам вооруженный эскорт. В этих случаях, принятие или отказ от эскорта могут зависить от того, считаете ли вы государство ответственным за безопасность правозащитников - но, в любом случае, правительство не может заявить о снятии с себя ответственности в случае отказа правозащитников от вооруженной охраны. Частные агентства охраны могут увеличить риск, если они неформально связаны с государственными силами правопорядка (см. Главу 9). Следует также отметить, что ношение личного оружия правозащитниками обычно неэффективно против организованных нападений, кроме того, это может повысить уязвимость правозащитников, если правительство использует это как повод для нападения на них под предлогом борьбы с терроризмом или мятежом.

Угрожающие ситуации, которые могут привести к нападению, легче урегулировать, если в неё вовлечены иные взаимодействующие персонажи и заинтересованные стороны. В качестве примера можно привести нормально функционирующую судебную систему; связи с организациями поддержки (внутри страны и за рубежом), которые могут оказать политическое давление на организаторов нападения; связи с общественными организациями, личные или семейные связи, связи с международными миротворческими подразделениями или войсками ООН и т.д.

Слежка и контрнаблюдение

Контрнаблюдение может быть полезным при определении, ведется ли за вами слежка. Трудно установить с точностью, ведется ли прослушивание ваших средств связи, поэтому всегда следует исходить из худшего[5]. Тем не менее, возможно определить, ведется ли слежка за вашими передвижениями и местом вашей работы.

4 Тем не менее, будут случаи, когда попытки уехать могут увеличить риск для кого-либо ещё.
5 Подробные сведения, касающиеся безопасности средств связи изложены в Главе 12.

Кто может следить за вами?

Люди, которые обычно находятся в вашей зоне, такие как швейцары или портье, курьеры внутри здания, уличные торговцы, работающие вблизи входов в здание, люди в припаркованных неподалёку автомобилях, посетители и т.д. - все они потенциально могут следить за вашими действиями. Люди могут вести слежку за деньги, под давлением и добровольно, либо по нескольким из этих причин сразу. Организаторы слежки могут также разместить своих сообщников или членов своей организации на вашей территории.

Слежка за вами может также вестись издали. В этом случае, следящие люди почти всегда члены какой-либо организации. Они, скорее всего, придерживаются тактики дистанционного наблюдения и не хотят, чтобы их заметили. Это означает соблюдение определенной дистанции, смену наблюдателей и наблюдение с различных точек, применение различных автомобилей и т.д.

Как определить, ведется ли за вами слежка

Вы можете определить наличие слежки путем наблюдения за теми, кто может следить за вами и при соблюдении следующих правил (безусловно, не впадая в паранойю):

- Если у вас есть основания считать, что кто-то, возможно, хочет проследить за вами, то вы должны быть внимательны к передвижениям людей на вашей территории и к изменениям в их поведении, например, если они начинают расспрашивать о вашей работе. Помните, что наблюдение могут вести не только женщины и мужчины, но также старики и подростки.

- Если вы подозреваете, что за вами следят, то можно воспользоваться контрнаблюдением с участием третьей стороны, которой вы доверяете и которая неизвестна тем, кто, возможно, ведет за вами наблюдение. Эта третья сторона может вести наблюдение - с упреждением и с достаточного расстояния - за всем, что происходит в период вашего прихода куда-либо либо ухода оттуда. Тот, кто ведет за вами наблюдение, скорее всего, будет это делать это в таком месте, где вас можно легко отыскать, включая ваш дом и места работы.

Пример

Перед приездом домой, вы можете попросить кого-либо из членов вашей семьи или соседа, которому вы доверяете, занять позицию для наблюдения в непосредственной близости от дома (например, заменяя колесо на автомобиле), чтобы проверить, ожидает ли кто-нибудь вашего появления. То же самое можно проделать, когда вы уходите из офиса пешком. Если вы пользуетесь частным автомобилем, то необходимо, чтобы другая машина следовала за вами, что даёт потенциальным наблюдающим за вами лицам возможность приблизиться к вам.

Преимущество контрнаблюдения состоит в том, что - пусть только в самом начале - лицо, ведущее за вами слежку, не подозревает, что вы о ней знаете. Поэтому все участники контрнаблюдения должны четко понимать, что открытое противодействие тем, кто ведет за вами слежку, нецелесообразно, так как им станет понятно, что вы знаете о ней, и это может спровоцировать насилие. При обнаружении слежки, очень важно принять все меры предосторожности и соблюдать дистанцию. При обнаружении слежки, вы можете принять необходимые меры, рекомендуемые настоящим Пособием (см. Главу 9).

Большинство этих рекомендаций по контрнаблюдению относятся практически исключительно к городским и полугородским районам. В сельской местности – всё по-другому: правозащитники и местные жители более восприимчивы к появлению незнакомых людей. Поэтому, тем, кто хочет организовать за вами слежку, труднее вести её на виду у жителей сельской местности, за исключением случаев, когда оно настроено враждебно по отношению к вашей работе.

Примечание: В некоторых случаях развитие отношений с сотрудниками сил безопасности, ведущими за вами наблюдение, может иметь свои преимущества, а в некоторых случаях слежка и вовсе намеренно ведётся в открытую - с целью запугивания. В некоторых случаях, правозащитники налаживают общение с сотрудниками сил безопасности, которые сообщают им о времени планируемой слежки либо нападения.

Когда проверять ведется ли за вами слежка

Логика подсказывает, что это разумно сделать тогда, когда у вас есть основания полагать, что за вами следят – например, в результате с инцидента, связанного с безопасностью. Если ваша работа по правам человека несет в себе определенный риск, то целесообразно время от времени проводить простые учебные контрнаблюдения.

Вы также должны подумать о том риске, который вы навлекаете на других в случае слежки за вами – риск может быть выше для свидетелей/членов семьи пострадавшего, с которыми вы встречаетесь, чем для вас – подумайте о наиболее безопасном месте встречи с ними. Возможно, вам следует предупредить их о том, что за вами может вестись наблюдение.

Реакция на нападения

Общего правила реагирования на все виды нападений на правозащитников не существует. Нападения также относятся к инцидентам, связанным с безопасностью, и в Главе 4 вы можете найти общие рекомендации о том, как на них реагировать.

При любом нападении важно помнить о двух следующих моментах:

- Всегда помните о безопасности! – как в процессе нападения, так и после него! (если вы подверглись нападению и вам необходимо сделать выбор между двумя альтернативными вариантами, сделайте его в пользу наиболее безопасного!).

- После нападения необходимо восстановиться физически и психологически, принять меры по нормализации ситуации и восстановить безопасные условия работы для вас и вашей организации. Очень важно сохранить как можно более подробную информацию о нападении: что именно произошло, кто/сколько человек в нем участвовало, номерные знаки автомобилей, описания участников и т.д. Эти данные необходимы для регистрации этого происшествия, и делать это следует как можно скорее. Полезно зарегистрировать этот случай и как можно быстрее собрать весь материал по нему. Храните копии всех документов по делу, переданных вами соответствующим органам для принятия мер.

Разработка стратегии и плана мероприятий по безопасности

Цель

Знакомство с принципами разработки стратегии безопасности и плана мероприятий по безопасности.

Правозащитники, работающие во враждебном окружении

Очень часто правозащитники работают во враждебном окружении. Этому есть множество объяснений. Большинство из них связано с тем, что работа правозащитников может привести их к конфронтации с могущественными персонажами, нарушающими международные законы о правах человека, в правительстве, в государственных органах власти, в органах безопасности, в оппозиционных вооруженных группировках или в независимых вооруженных бандах. Эти лица могут нанести ответный удар и попытаться заставить правозащитников прекратить свою работу, используя при этом различные средства - от скрытого ущемления свободы выражения до угроз и прямых нападений. Степень терпимости этих персонажей зависит от характера работы правозащитников: определённые действия могут быть расценены как приемлемые, другие - нет. Зачастую такая неопределенность носит умышленный характер.

Здесь уместно сказать о двух важных моментах: Во многих случаях только определенные элементы **в** среде коллективных персонажей (о которых говорилось выше) относятся враждебно к правозащитникам. Например, некоторые элементы, входящие в состав правительства, могут относиться к защите правозащитников сравнительно серьезно, в то время как другие могут быть склонны к агрессии против них. Кроме того, правозащитники могут испытывать большую враждебность в периоды политической нестабильности, например, выборов либо иных политических событий.

Социо-политическое рабочее пространство правозащитников

Настоящее Пособие рассматривает защиту и безопасность правозащитников, работающих во враждебной среде, и меры, направленные на повышение их безопасности. Для повышения уважения к правам человека и улучшения внешней среды, в которой находятся правозащитники, необходимо также принятие соответствующих мер на социо-политическом уровне. Проведение кампаний и мероприятий по популяризации деятельности правозащитников часто направлено на достижение более широкого признания прав человека в обществе или на то, чтобы добиться от властей принятия более эффективных мер по их защите. При этом, мы, как правило, не задумываемся о безопасности, но если она соблюдается, то это может оказать позитивное влияние на **социо-политическое рабочее пространство** правозащитников.

Это социо-политическое рабочее пространство можно определить как **многообразие действий, которые правозащитник может предпринять при допустимом уровне личного риска.** Другими словами, правозащитник осознает "широкий выбор возможных политических действий и соотносит их с возможными издержками либо последствиями". Часть этих последствий правозащитник воспринимает как "приемлемые, а остальные - как неприемлемые, определяя, таким образом, границы существующего политического пространства".

Например, группа правозащитников может вести дело о защите прав человека до тех пор, пока кто-то из членов группы не получает угрозу быть убитым. Если группа считает, что у неё достаточно социо-политического пространства, то она может решить предать угрозу гласности и, в итоге, продолжить свою работу. Но если она считает, что её политическое пространство ограниченно, она может решить, что осуждение угрозы повлечет неприемлемые последствия. Группа может даже принять решение прекратить дело на некоторое время, дабы улучшить свою безопасность.

Понятие "приемлемый" риск может изменяться со временем и в зависимости от того относиться ли оно к отдельным лицам либо к организациям. Например, для некоторых пытки или смерть члена семьи могут быть совершенно недопустимым риском. Некоторые правозащитники считают, что заключение их в тюрьму является приемлемым риском, если это способствует достижению целей. Для других лимит риска может быть исчерпан первой же угрозой в их адрес.

Это политическое пространство деятельности, помимо субъективных определений его самими участниками действий, очень чувствительно к изменениям окружающей национально-политической среды. Поэтому вы должны рассматривать его как пространство относительное и изменчивое.

Безопасность и рабочее пространство правозащитников

Все стратегии безопасности можно кратко подытожить как желание расширить своё рабочее пространство и поддерживать его в этом состоянии. Строго говоря, с точки зрения безопасности, рабочее пространство правозащитника требует, по меньшей мере, минимального уровня согласия основных персонажей данного региона, особенно политических и военных властей и вооруженных групп, интересы которых могут пострадать в результате деятельности правозащитников и которые способны принять решение о действиях против них.

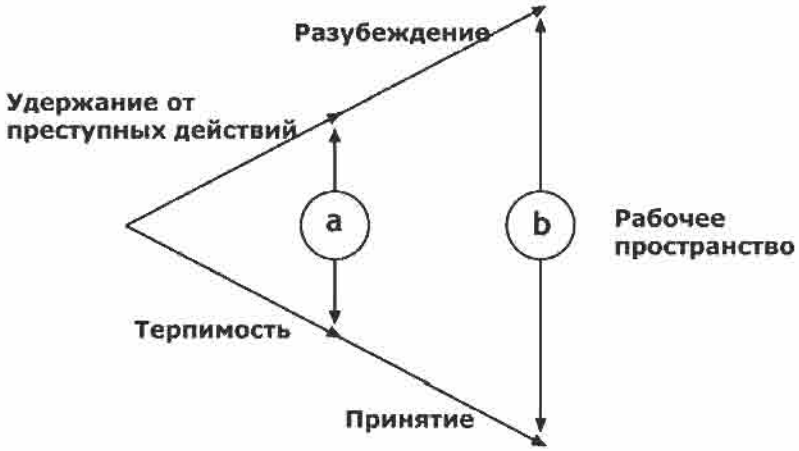
Это согласие может быть **явным**, в виде формального разрешения властей, или **завуалированным**, например, в случае с вооруженными группами. Согласие будет весомее, если персонаж его дающий может усматривать в работе правозащитников какие-либо выгоды для себя. И менее весомым, если он увязывает вашу работу с издержками для себя. В этом случае, степень его согласия будет зависеть от политических издержек, связанных с организацией нападения на правозащитников. Эти вопросы особенно актуальны при вооруженных конфликтах, когда правозащитники сталкиваются с несколькими вооруженными персонажами. Приемлемость деятельности правозащитников для одного из персонажей может вызвать враждебность у его оппонента.

Рабочая среда правозащитников может быть представлена двумя осями:

- одна из них обозначает предел, до которого персонаж будет мириться с вашей работой – в зависимости от степени влияния вашей деятельности на его цели или стратегические интересы (континуум терпимость-принятие).

1 Это определение и другие основные элементы данной концепции заимствованы у Махони и Эгурена (Mahony & Eguren, 1997; p. 93), которые разработали также модель политического пространства, включающего рабочую среду правозащитника и защитное сопровождение правозащитников.

- другая обозначает предел, до которого вы способны сдерживать акты насилия и который увеличивается, если с помощью рациональных/моральных аргументов вам удается разубедить персонаж либо даже убедить его в политических выгодах отказа от нападения на вас или нарушения прав человека по причине



больших политических издержек (континуум сдерживание-разубеждение). Расширения вашего рабочего пространства можно добиться и с течением времени. Для достижения приемлемости работы правозащитников путем стратегии разубеждения, следует учитывать интересы населения, ваш имидж, существующие процедуры, интеграцию и т.д., как показано в части "b". Но в зонах вооруженных конфликтов рабочее пространство обычно ограничивается участком, определяемым согласием вооруженных персонажей, частично продиктованным издержками нападения на правозащитников (разубеждение) и затем уменьшенным до величины "a".

Расширение вашего рабочего пространства путем повышения терпимости и приемлемости

Ваша работа может воздействовать на цели либо стратегические интересы тех, кого мало интересуют права человека, и тем самым привести к возникновению враждебной рабочей среды для правозащитников. Для того, чтобы добиться приемлемости или, по крайней мере, согласия на её проведение, важно ограничить конфронтацию до необходимого минимума. Вот несколько советов о том, как этого добиться:

- **Наладить обучение и распространение информации о характере и законности работы правозащитников.** Правительственные чиновники и другие высокопоставленные лица, возможно, проявят большую склонность к сотрудничеству, если они знают и понимают вашу работу, а также причины, по которым вы её проводите. Недостаточно ознакомить с вашей работой лишь высокопоставленных официальных лиц, поскольку в повседневности правозащитники обычно имеют контакты с представителями правительственных органов различного уровня. Вы должны постоянно информировать и обучать официальных представителей на всех уровнях правительства.
- **Разъяснять цели работы правозащитников.** Во всех конфликтах полезно разъяснять и чётко обозначать масштабы и цели вашей работы.

Это позволит снизить уровень непонимания или ненужной конфронтации, которые могут помешать правозащитникам достичь своих целей.

- **Ограничьте цели вашей работы в соответствии с её социо-политическим пространством.** Когда работа правозащитников напрямую затрагивает важные стратегические интересы вооруженного персонажа, то он может отреагировать с большей агрессивностью и с меньшим учетом ущерба для своего имиджа. Некоторые виды работы делают правозащитников более уязвимыми, чем другие, поэтому убедитесь, что ваши цели максимально согласуются с вашим риском и с вашими возможностями защиты.

- **Обеспечьте своим стратегиям гибкость с целью "сохранения доброго имени".** Если вам придется вступить в конфронтацию с влиятельными лицами по вопросам нарушения прав человека, постарайтесь оставить им шанс для сохранения своей репутации и принятия мер по урегулированию ситуации.

- **Обзаведитесь союзниками** в максимально возможном числе общественных прослоек.

- **Найдите золотую середину** между прозрачностью вашей работы, чтобы показать, что легитимным правозащитникам нечего скрывать, и необходимостью избегать предоставления информации, которая может скомпрометировать вашу работу или безопасность.

- **И, наконец,** помните, что легитимность и качество вашей работы являются необходимыми условиями для поддержания её пространства открытым, но одного этого недостаточно. Возможно, от вас также потребуется умение разубеждать потенциальных организаторов нападения (см ниже).

Расширение вашего рабочего пространства: расширение сдерживания и разубеждения.

Правозащитники, работающие во враждебном окружении, должны быть в состоянии запугать агрессора достаточным количеством возможных для него политических издержек с целью его отказа от нанесения удара. Это и называется **сдерживанием**.

Полезно провести различие между "общим" и "немедленным" сдерживанием**. Общее сдерживание** подразумевает общий результат действия всех общенациональных и международных усилий по защите правозащитников, т.е. всего того, что способствует формированию общественного мнения о том, что акты агрессии против правозащитников будут иметь негативные последствия. Эти усилия могут осуществляться путем проведения широких тематических кампаний, либо путем обучения и распространения информации о защите правозащитников. С другой стороны, **немедленное сдерживание** представляет собой направление специфической информации конкретному агрессору для предупреждения нанесения удара по специфической цели. Немедленное сдерживание необходимо, когда общее сдерживание не дает результатов или представляется недостаточным, а также тогда, когда усилия по защите сфокусированы на специфических объектах.

Разубеждение представляет собой более ёмкую концепцию. Её можно определить как результат мер, направленных на оппонента с целью побудить его отказаться от выполнения задуманного враждебного акта. Убедительная аргументация, призыв к нравственности, расширение сотрудничества, развитие межличностного взаимопонимания, ваша неагрессивная манера держаться, отвлечение внимания – все эти приёмы можно использовать для достижения эффекта разубеждения. Кроме того, для успешного разубеждения можно также использовать политику примирения и сдерживания. Каждая из этих тактик в разное время применяется правозащитниками на национальном и международном уровне. Естественно, правозащитники не могут очень часто прибегать к прямым "угрозам": их стратегия скорее сводится к тому,

чтобы напомнить другим, что, в зависимости от их решений, их действия **могут** вызвать некие последствия.

Применение тактики сдерживания

Чтобы определить, была ли тактика сдерживания эффективной, необходимо выполнить ряд условий:

1 •**Правозащитники должны четко сформулировать и сообщить агрессору, какие именно действия являются неприемлемыми.** Тактика сдерживания не принесёт результатов, если агрессор точно не знает, какие именно его действия вызовут обратную реакцию.

2 •**Правозащитная организация должна сформулировать свою позицию по сдерживанию агрессора таким образом, чтобы она была понятна агрессору.** Организация также должна иметь готовую стратегию для осуществления сдерживания.

3 •**Правозащитная организация должна быть способна претворить в жизнь тактику сдерживания и заставить агрессора поверить в это.** Если "угроза" обеспечения общенациональной или международной реакции нереальна, то нет оснований считать, что она остановит агрессора.

4 •**Правозащитники должны точно знать, кто является агрессором.** Банды наёмных убийц, к примеру, часто работают под покровом ночи и редко берут на себя ответственность за преступления. Поэтому всё сводится к анализу, кому это нападение могло бы быть выгодно. Для эффективности общенациональной или международной реакции на события, даже вполне оправданное утверждение об "ответственности за них государства" требует более конкретной информации о том, какие именно группировки в государственном аппарате стоят за нападением.

5 •**Необходимо учитывать возможность того, что агрессор,** серьезно рассмотрев нападение как вариант, решил отказаться от него, так как цена агрессии – благодаря действиям правозащитников – перевесит получаемые им выгоды.

Правозащитникам трудно разубедить агрессора, на которого их намерения прибегнуть к тактике сдерживания не производят никакого воздействия: это происходит в тех случаях, когда правительство может быть наказано международным сообществом, но само не в состоянии наказать конкретных нарушителей прав человека. Например, частные армии могут быть вне правительственного влияния, или не разделять его интересов. В этих случаях агрессор может даже выиграть он нападения на правозащитников, потому что эти нападения поставят правительство в трудное положение и нанесут ущерб его репутации.

Правозащитники никогда не могут знать заранее, будут ли их "аргументы по сдерживанию агрессора" достаточно убедительными, чтобы предотвратить потенциальное нападение. Агрессор может рассчитывать на выгоды, о которых правозащитники могут не знать. Оценка ситуации с максимальной тщательностью представляет собой постоянную задачу, которая может быть невыполнимой по причине отсутствия наиважнейшей информации. Организации правозащитников должны, таким образом, разрабатывать чрезвычайно гибкие планы отхода и способности быстрого реагирования на непредвиденные обстоятельства.

Подготовка плана безопасности

Составление плана безопасности не представляет трудности. Этот процесс включает всего лишь несколько стадий:

1 • **Компоненты плана.** План безопасности предназначен для снижения вашего

риска. Поэтому он должен преследовать, по меньшей мере, три цели, основанные на вашей оценке риска:

- Снижение уровня полученной вами угрозы.
- Снижение вашей уязвимости.
- Расширение ваших способностей к защите.

Будет полезно, если ваш план также будет включать:

- Превентивные планы или правила выполнения повседневной работы в соответствии с нормами безопасности, например, того, как подготовить публичное заявление или посещение удаленного района.

- Чрезвычайные планы для урегулирования конкретных проблем, например, ареста либо похищения.

2 • **Распределение обязанностей и ресурсов для реализации плана.** Для гарантии выполнения плана ваша повседневная работа должна вестись с соблюдением общепринятых правил безопасности:

- Постоянно включайте оценку контекста и вопросы безопасности в повседневные программы вашей работы.
- Регистрируйте и анализируйте инциденты, связанные с безопасностью.
- Распределите обязанности.
- Распределите ресурсы, т.е. время и денежые средства, для сохранения вашей безопасности.

3 • **Составление плана – с чего начать.** Если вы провели оценку риска для отдельного правозащитника или организации, то у вас может появиться длинный перечень уязвимых мест, несколько видов угроз и ряд ресурсов . Практически, всё это вы можете сделать одновременно. Итак, с чего начать? Это очень просто:

- **Выберите несколько угроз.** Расположите выбранные угрозы в порядке их приоритета, независимо от того, являются ли они фактическими или потенциальными, используя один из следующих критериев: к примеру, овершенно очевидно, что наиболее серьёзную угрозу представляют угрозы убийст ИЛИ наиболее серьезная и вероятная угроза - если нападению подвергаются организации аналогичные вашей, то значит такая угроза потенциально опасна и для вас; ИЛИ это угроза, которая теснее всего связанна с вашими уязвимыми местами - поскольку именно в них риск становится максимальным.

- **Составьте перечень своих уязвимых мест, соответствующих угрозам, которые вы внесли в список.** В первую очередь, необходимо обратить внимание на уязвимые места, но помните, что не все уязвимые места связаны с угрозами. Например, если вы получили угрозу убийства, то вряд ли вам поможет, если вы начнёте запирать шкафы в вашем офисе в центре города (за исключением случаев, когда вы можете легко подвергнуться нападению в офисе, что обычно маловероятно). Поэтому было бы более целесообразно снизить вашу уязвимость при поездке из дома в офис или в выходные дни. Запирание шкафов само по себе, вероятно, не снизит вашу уязвимость перед лицом угрозы убийства.

- **Составьте перечень своих ресурсов, соответствующих угрозам, которые вы внесли в список.**

Теперь в вашем плане безопасности вы можете учесть выбранные угрозы, уязвимые места и ваши ререурсы защиты, и у вас есть веские основания быть уверенными в том, что вы сможете снизить ваш риск на самом начальном этапе.

Помните, что это целенаправленный способ составления плана безопасности.

Существуют также более "формальные" способы составления планов безопасности, но этот метод является наиболее прямым и обеспечивает принятие мер по самым неотложным проблемам безопасности, при условии, что ваша оценка риска верна, и, в конечном итоге, позволяет разработать "жизнеспособный" и "реальный" план, а это важная часть безопасности. (Подробный перечень возможных компонентов планов безопасности, которые вы также можете использовать при оценке ваших рисков, вы найдёте в конце данной главы).

Решение проблем безопасности: Поэтапное управление безопасностью

Управление безопасностью не заканчивается никогда и всегда является частичным и избирательным. Это происходит по следующим причинам:

- Существуют предельные объемы информации, с которой вы можете работать – не все факторы, влияющие на безопасность, можно классифицировать и анализировать одновременно.

- Это сложный процесс – для достижения понимания требуется время и усилия, достижение единомыслия, обучение людей, решение вопросов, связанных с текучестью кадров, реализация мероприятий и т.д.

Управление безопасностью прагматично

Управление безопасностью редко может претендовать на всесторонний, долгосрочный анализ. Её значимость состоит в способности предотвратить нападения и указать на необходимость организационных стратегий для борьбы с агрессией. Это может показаться не очень амбициозным, но мы не должны забывать, что, как правило, на безопасность выделяются черезчур ограниченные ресурсы!

При анализе практики безопасности отдельного правозащитника или организации, вы можете обнаружить некоторые инструкции, планы, мероприятия или модели поведения. Они могут выглядеть противоречивыми - от стереотипных идей о практике защиты до нежелания увеличивать существующие рабочие нагрузки, неизбежные при включении новых мероприятий по безопасности.

Практика защиты обычно представляет собой фрагментированную и интуитивную деятельность в процессе её развития. Управление безопасностью должно быть направлено на поэтапные изменения с целью совершенствования её эффективности. Правила и процедуры безопасности обычно появляются в результате деятельности различных подразделений, работающих в специфических направлениях. Группы, связанные с материально-техническим обеспечением и выездом на места, особенно заинтересованы в своей безопасности, так же как и руководитель, находящийся под давлением своих финансовых доноров.

Шаг за шагом, управление безопасностью открывает двери неформальным процессам и освобождает место для внедрения новой практики. Неожиданные события, такие как инциденты, связанные с безопасностью, требуют принятия немедленных, краткосрочных решений, которые при хорошем управлении позволят сформировать более долгосрочную практику безопасности для всей организации.

Выполнение плана безопасности

Планы безопасности важны, но их не так просто выполнить. Выполнение плана пресдтавляет собой нечто гораздо большее, чем простой технический процесс – это процесс организационный, что означает поиск не только начальных точек и возможностей, но также - барьеров и проблем.

План безопасности должен быть выполнен, по меньшей мере, на трёх

уровнях:

1 • На **индивидуальном** уровне. Для того чтобы план мог быть реализован, ему должен следовать ть каждый член оргпнизации.

2 • На **организационном** уровне. Организация в целом должна следовтаь плану.

3 • На **межорганизационном** уровне. Для обеспечения безопасности обычно требуется определенный уровень сотрудничества между различными организациями.

Примеры начальных моментов и возможностей при выполнении плана безопасности:

- Произошло несколько незначительных инцидентов, связанных с безопасностью, в вашей или иной организации и некоторые члены организации обеспокоены этим.
- В связи с ситуацией в стране, безопасность вызывает определенное беспокойство.
- Прибывают новые сотрудники, и после их подготовки можно с большей легкостью начать использовать более эффективную практику защиты.
- Другая организация предлагает вам обучение по проблемам защиты.

Примеры проблем и барьеров при выполнении планов по безопасности:

- Некоторые люди считают, что дополнительные меры безопасности приведут к ещё большей рабочей нагрузке.
- Некоторые люди думают, что организация уже имеет достаточную безопасность.
- "У нас нет времени на эти мелочи!"
- "Хорошо, давайте найдем дополнительное время и обсудим вопросы безопасности в субботу утром, и кончено!"
- "Нам нужно больше заботиться о тех людях, которым мы собираемся помочь, а не о себе."

Способы улучшения внедрения плана безопасности

- **Воспользуйтесь возможностями и исходными данными** для решения проблем и устранения барьеров.
- **Продвигайтесь шаг за шагом.** Не стоит делать вид, что всё можно сделать сразу.
- **Подчеркните важность всеобъемлющей безопасности с точки зрения пострадавших.** Подчеркните, что безопасность свидетелей и членов их семей чрезвычайно важна для эффективности работы, и что этим процессом лучше всего управлять через интегрирование надежной практики безопасности во все сферы деятельности. Используйте при обучении/обсуждении примеры, демонстрирующие потенциально негативное влияние отсутствия безопасности на свидетелей и пострадавших.

- План, подготовленный двумя "экспертами" and presented to a whole organisation is lik План, подготовленный двумя "экспертами" и представленный всей организации, может не сработать. В безопасности **ключевым моментом является массовое участие.**

- **План должен быть реальным и выполнимым.** Длинный перечень того, что нужно сделать перед выездом на место событий, не принесет результатов. Довольствуйтесь минимумом, необходимым для обеспечения безопасности. Это ещё один аргумент в пользу привлечения тех, кто реально выполняет работу – например, сотрудников, которые часто посещают места событий.

- **План – это не какой-то одноразовый документ**, он всё время должен пересматриваться и обновляться.

- **План следует рассматривать не как "дополнительную работу", а как "улучшенный метод работы".** Люди должны видеть его реальные преимущества, например, предотвращение дублирования отчетов. Убедитесь, что отчеты о поездках на места событий подготовлены в свете безопасности; вопросы безопасности должны стать частью обычных совещаний группы, включите элементы безопасности в другие виды обучения и т.д.

- **Подчеркните, что безопасность – это не личный выбор.** Индивидуальные решения, отношение и поведение, влияющие на безопасность, могут иметь последствия для защиты свидетелей, членов семей пострадавших и ваших коллег. Внедрение надежной практики безопасности возможно только при коллективном устремлении.

- **Необходимо распределить время и ресурсы для выполнения плана**, так как повышение безопасности за счёт свободного времени людей не приемлемо. Чтобы сотрудники рассматривали меры безопасности как важные, они должны сочетаться с другими "важными" мероприятиями.

- **Контролировать соблюдение плана всеми**, особенно руководителями и теми, кто несет ответственность за работу других людей. Те, кто упорно отказывается от соблюдения плана, должны нести за это ответственность.

Возможные элементы плана безопасности

Это "меню" дает подробный перечень элементов безопасности для включения в план. После оценки риска вы можете воспользоваться приведенными ниже советами для составления вашего собственного плана безопасности.

- Назначение организации, миссия и общие цели.

- Организационное определение политики безопасности.

- Вопросы безопасности должны сочетаться со всеми аспектами повседневной работы, такими как: контекстная оценка, оценка риска и анализ инцидентов, а также оценка безопасности.

- Хороший план, дающий ответ на вопросы о том, как добиться, чтобы весь персонал имел достаточный уровень подготовки по безопасности и как обеспечить преемственность функций по безопасности в случае, если какие-либо сотрудники покинут организацию.

- Распределение обязанностей: Кто за что отвечает в какой-либо ситуации?

- Как справится с кризисом безопасности: Создать кризисную комиссию или рабочую группу с возложением на нее обязанностей по взаимодействию со средствами массовой информации, по связям с родственникам и т.д.

- Обязанности организации: Планирование, контроль выполнения, страхование, гражданская ответственность и т.д.

- Обязанности каждого сотрудника: Стремиться снизить риск в период свободного времени и на отдыхе, сообщать и регистрировать инциденты, связанные с безопасностью, санкции (некоторые из этих элементов можно включить в рабочие контакты, если это целесообразно).

- Политика организации по следующим вопросам:

  1-Отдых, свободное время и управление стрессами. 2-Серьезные инциденты, такие как похищение, исчезновение, причинение телесных повреждений и т.д. 3-Охрана свидетелей. 4-Предупреждение заболеваний и несчастных случаев. 5-Связи с властями, силами безопасности и вооруженными группировками. 6-Управление и хранение информации, обращение с секретными документами и информацией. 7-Ваш личный престиж в отношении религиозных, социальных и культурных ценностей. 8-Управление безопасностью в офисах и жилых помещениях (в том числе и для посетителей).

- Планы профилактики и прочие правила:

  1-Подготовка выездов на места событий. 2-Обращение с деньгами и ценностями. 3-Средства связи и протокол. 4-Обслуживание автотранспорта. 5-Мины. 6-Снижение риска быть вовлечённым в обычные правонарушения, вооруженные инциденты или преступления на сексуальной почве. 7- Снижение риска несчастных случаев в дороге или в зонах риска.

- Планы и правила реагирования на кризисы безопасности, такие как:

  1- Экстренные медицинские и психологические проишествия (также на местах событий). 2-Нападения, включая преступления на сексуальной почве. 3-Грабежи. 4-Реагирование на неявку человека в назначенное время. 5-Арест или задержание. 6-Похищение. 7-Пожар и другие несчастные случаи. 8-Эвакуация. 9-Стихийные бедствия. 10-Санкционированные либо несанкционированные обыски, ограбления офиса либо жилых помещений. 11-Попадание под обстрел. 12-Убийство. 13-Государственный переворот.

Оценка эффективности системы безопасности в вашей организации: колесо безопасности

Цель

Анализ вашего способа управления безопасностью.

Оценка глубины интегрирования безопасности в работу правозащитников.

Колесо безопасности

Начнем с простого: для нормального вращения, колесо должно быть абсолютно круглым, и это бесспорно. Но что происходит, если некоторые из спиц длиннее, чем другие? Колесо не будет абсолютно круглым и, поэтому, не будет функционировать надлежащим образом.

Нечто похожее происходит с управлением безопасностью в группе или организации. Если основные её элементы не развиваются одновременно, то и вся стратегия не может функционировать нормально. На этом основании, вы можете набросать эскиз так называемого "колеса безопасности". Вы можете использовать его для анализа того, как вы управляете безопасностью и для оценики степени интегрирования безопасности в работу группы правозащитников.

Эту оценку можно выполнять группой. Вы можете назвать множество причин, из-за которых определенные части колеса не были развиты в достаточной мере, и предложить различные способы решения этих проблем. После предложения возможных решений, вы можете приступить к работе и выбрать те из них, которые вы намереваетесь использовать.

После оценки вашего колеса безопасности, перенесите полученные результаты на диаграмму. Когда вы повторите этот анализ несколько месяцев спустя, вы сможете сравнить вашу старую диаграмму с новой и проследить пункт за пунктом, улучшилась ли ситуация или наоборот.

Компоненты колеса безопасности

Колесо безопасности имеет восемь спиц, либо компонентов:

- **Опыт на рабочем месте:** Практические знания по безопасности и защите. Ваша точка отправления и прибытия.

- **Обучение.** Вы можете получить подготовку по безопасности на курсах или по собственной инициативе в ходе вашей повседневной работы.

- **Осведомленность о безопасности и отношение к ней:** Связаны с тем, действительно ли каждый член организации и организация в целом рассматривают безопасность как необходимость и готовы ли они к её обеспечению

- **Планирование:** Способность планирования безопасности и работы. Планирование защиты.

- **Распределение обязанностей:** Кто именно отвечает за те или иные аспекты безопасности и защиты? Кто именно отвечает за те или иные аспекты безопасности и защиты в критических ситуациях?

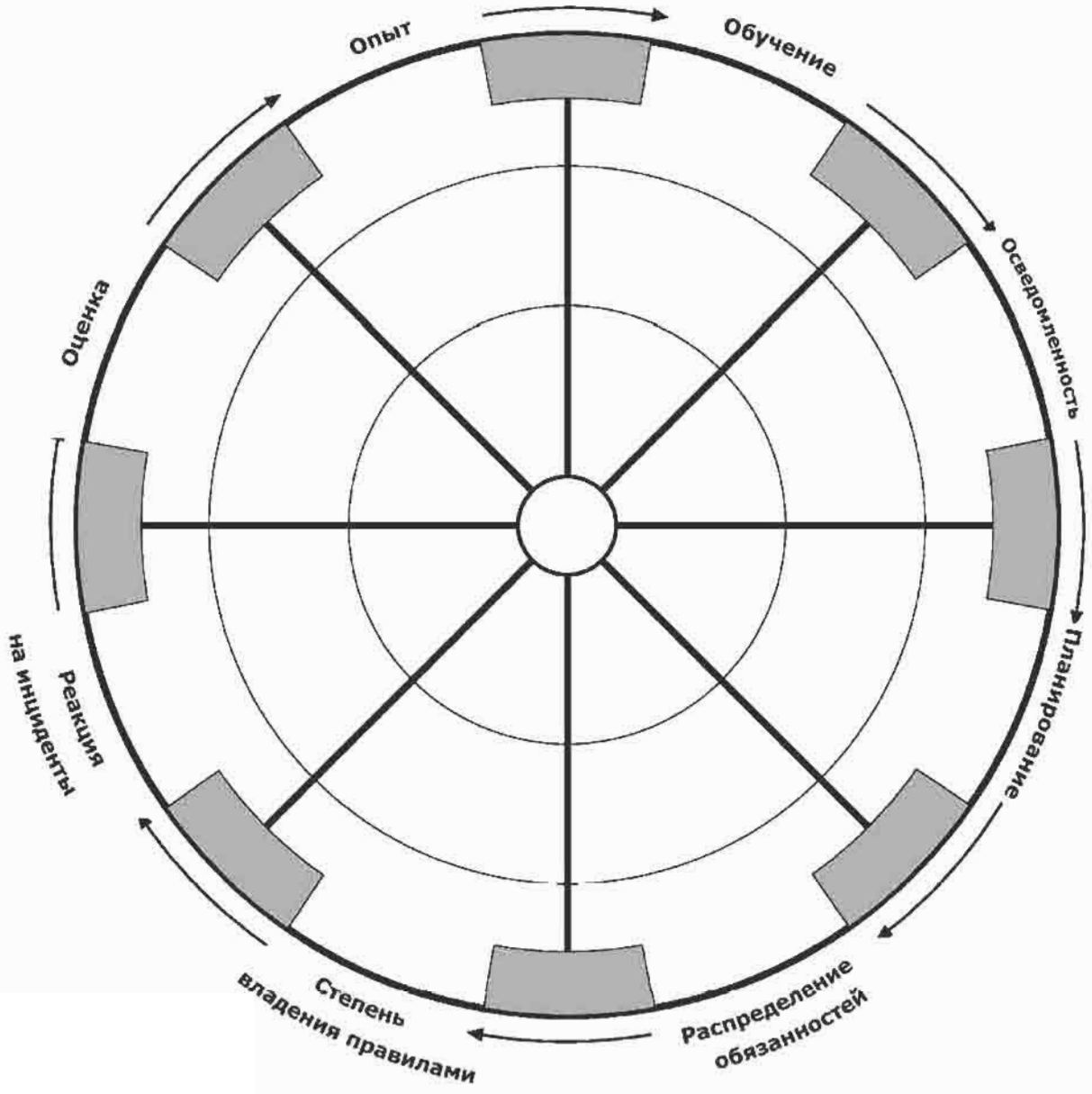
- **Степень владения правилами безопасности / их соблюдение:** В какой мере люди соблюдают правила и процедуры безопасности?

- **Анализ и реакция на инциденты, связанные с безопасностью:** В какой мерее анализируются инциденты, связанные с безопасностью? Насколько адекватна реакция на них в организации?

- **Оценка управления безопасностью и защитой:** Если вы производите оценку своей повседневной работы и реакции на инциденты, то это будет способствовать приобретению знаний и опыта отдельными сотрудниками и всей организацией правозащитников в целом.

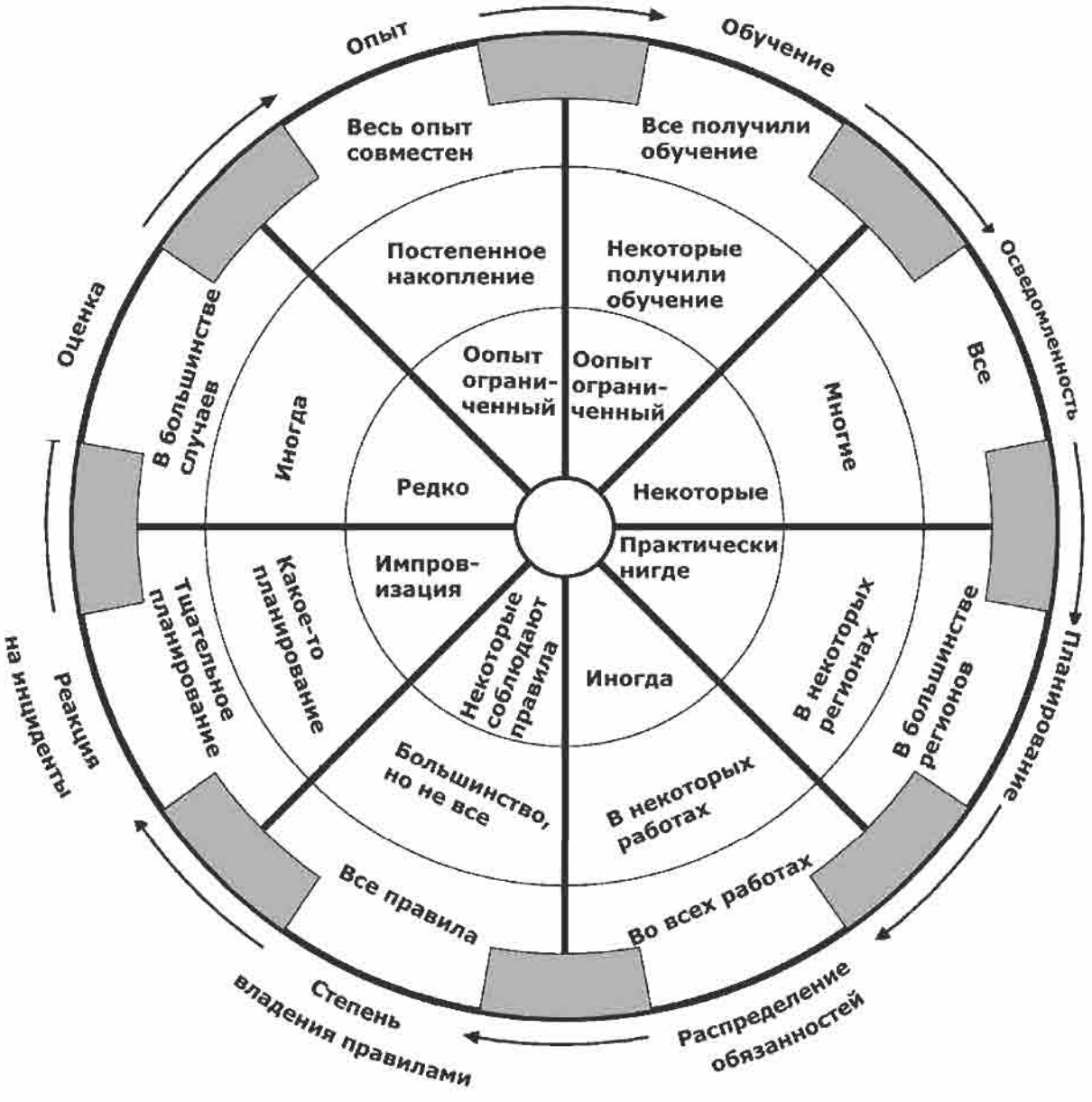
Теперь, конгда вы ознакомились с компонентами колеса безопасности, постарайтесь составить диаграмму и внести в неё дополнительную информацию. Она может выглядеть следующим образом:

Колесо безопасности и восемь составляющих его компонентов ("спиц")



Колесо безопасности никогда не достигает совершенства:

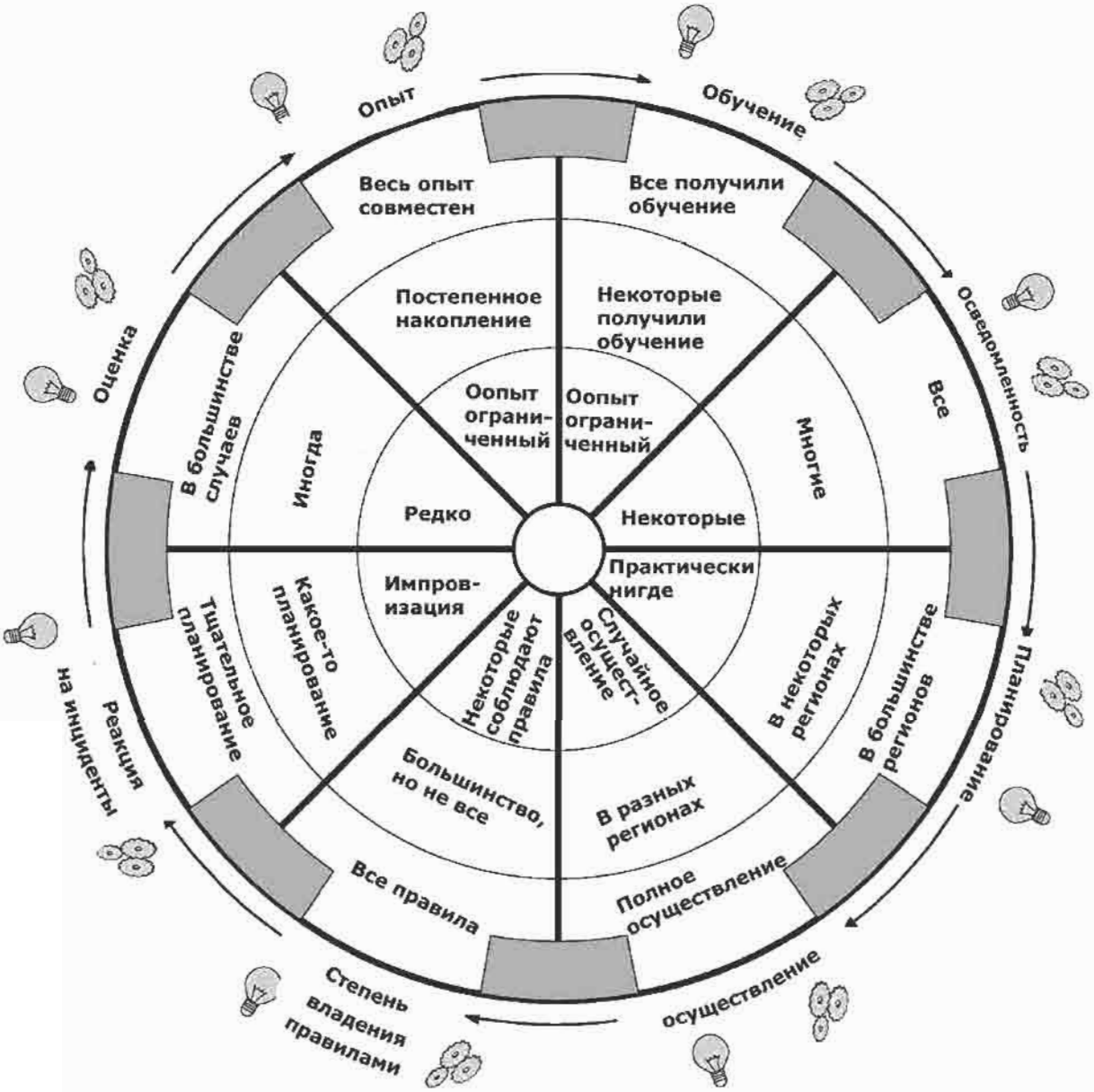
Некоторые его части более развиты, чем другие. Поэтому более целесообразно провести анализ степени развития каждой части. Таким образом, вы можете определить, каким видам действий вам следует уделять первостепенное внимание для совершенствования вашей защиты и безопасности. Каждая тонкая линия, идущая от центра, иллюстрирует степень развития определённого компонента колеса.



скопируйте колесо на бумагу или на цветную плёнку и раскрасьте участки между спицами. Это позволит вам представить истинную форму колеса безопасности вашей группы или организации и увидеть, какие его компоненты развиты больше, а какие меньше.

Если какой-либо из восьми компонентов колеса развит слабо, то вам следует определить:

Какие проблемы связаны с этой частью колеса ...
...и каковы варианты решения этих проблем.



Обеспечение соблюдения правил и процедур безопасности

Цель

Анализ причин, делающих персонал и организацию правозащитников неспособными или несклонными к соблюдению планов и процедур безопасности, и поиск соответствующих решений.

Безопасность касается всех

Вопрос о том, соблюдают ли отдельные правозащитники и их организации правила и процедуры безопасности, на практике является сложным. Вполне возможно иметь хороший план безопасности, включающий меры профилактики и правила поведения в критических ситуациях; вопросы безопасности могут считаться приоритетными при обсуждении на всех важных больших совещаниях и тем не менее, люди не обязательно будут их придерживаться.

Это может показаться невероятным, если вспомнить, что правозащитники постоянно находятся под давлением и им постоянно угрожают. Но это так.

Если кто-то наводит справки о вашей работе, то он не будет пытаться получить информацию от наиболее осторожных членов вашей организации. Скорее всего, он обратится к тем, кто, скажем, злоупотребляет спиртным. Точно так же, если кто-то хочет запугать вашу организацию, то он, вероятно, не нападет на сотрудника, принявшего все необходимые меры предосторожности. Скорее всего, его действия будут направлены на того, кто обычно не обращает внимания на собственную безопасность. Может случиться и так, что осторожный человек всё же подвергнется нападению, но лишь из-за того, что его беспечный коллега оставил дверь открытой … Суть в том, что беспечность одного может увеличить риск для всех остальных.

Поэтому безопасностьследует рассматривать как проблему всей организации, равно как и отдельных её членов. Если только 3 из 12 сотрудников соблюдают правила безопасности, то вся организация, включая и тех, кто эти правила соблюдает, ставится под угрозу. Если ситуация улучшается и девять человек начинают соблюдать правила безопасности, то риск снижается. Но риск будет намного меньше, если правила безопасности соблюдают все 12 человек.

Безопасность -
это вопрос не только каждого человека в отдельности,
но и всей
организации в целом.

Хороший план безопасности теряет смысл, если он не соблюдается. Давайте будем реалистами: многие люди не следуют правилам и процедурам безопасности. Это несоблюдение приводит к несоответствию между добрыми намерениями и их эффективностью в реальной жизни. Тем не менее, с самой этой проблемой значительно легче совладать, чем с её возможными последствиями.

Почему люди не соблюдают правила безопасности и как избежать этого изначально?

Прежде всего, слово "соответствие" подразумевает «подчинение» и «послушание», поэтому его следует избегать. Люди соблюдают только те правила, которые они понимают и принимают как свои собственные. Поэтому ключевым словом здесь является слово "владение".

Для того чтобы процедура безопасности соблюдалась, её должен принять каждый член организации. Но это происходит не сразу. Для того, чтобы персонал принял правила безопасности, он должен иметь возможность участвовать в их разработке и осуществлении. Обучение, понимание и принятие процедуры также являются принципиально важными.

Таблица 1: Связь между отдельными сотрудниками и организациями с позиции безопасности.

Концепция	Подход: " Каждый должен соблюдать правила!	Подход: " Члены организации и организация договорились о правилах!"
Подход	Нацеленный на правила	Основанный на потребностях безопасности личности и организации
Характер отношений между отдельным сотрудником и организацией	Нормативный или "покровительственный"	Основанный на диалоге
Почему мы соблюдаем правила?	В силу обязанности; для того, чтобы избежать санкций или увольнения	Для соблюдения соглашения, с долей критики и возможностью совершенствования (потому что мы согласны с целью/необходимостью, для того чтобы помочь защитить своих коллег и людей, с которыми мы работаем)
Ответственность за безопасность	Индивидуальная	Коллективная

Владение правилами безопасности означает не просто "соблюдение определенных правил", но и установление договоренности о правилах, побуждающей к их соблюдению, в силу понимания сотрудниками сути этих правил, их целесообразности и эффективности, а также осознания того, что это связано с их личной безопасностью. С этой целью, правила, в свою очередь, должны соответствовать моральным и этическим критериям, а также основным потребностям людей.

Владение правилами безопасности - это не просто "соблюдение правил", это осознание соглашения по безопасности между организацией и персоналом.

Для поддержания эффективности соглашения между членами организации и организацией в целом важно чтобы **лица, отвечающие за безопасность, постоянно привлекали остальных к решению этой проблемы,** проводя инструктажи, напоминая об аспектах соглашения и путем опроса мнений о том, насколько правильны и эффективны эти правила на практике.

Однако, такое участие принесёт мало пользы без **культуры безопасности в организации,** которая служит основой для формальных и неформальных процедур работы или программ.

Необходимый базис для соблюдения правила и процедуры безопасности, можно достичь путем принятия следующих мер:

- Развитие понимания о том, что безопасность важна для защиты жертв, свидетелей, членов их семей и их коллег для достижения основных целей работы, проводимой организацией.

- Развитие и оценка культуры безопасности организации.

- Углубление владения правилами и процедурами безопасности.

- Обеспечение участия всего персонала в разработке и совершенствовании правил и процедур безопасности.

- Обучение сотрудников приёмам безопасности.

- Обеспечение того, чтобы весь персонал был убежден в правильности и эффективности правил и процедур безопасности.

- Заключение соглашения между организацией и её членами о соблюдении правил и процедур безопасности.

- Привлечение лиц, ответственных за безопасность, к инструктажу и обучению сотрудников; к напоминанию персоналу об условиях соглашения и к опросу мнений о том, насколько правильны и эффективны эти правила на практике.

Почему не соблюдаются правила и процедуры безопасности

Не существует такого правозащитника, который вообще не соблюдал бы правил безопасности. Большинство соблюдают лишь определенные правила, да и то, как правило, от случая к случаю.

Существует множество причин несоблюдения правил и процедур безопасности. Для того чтобы это изменить, важно установить причины и найти решения вместе с теми, кого эти проблемы касаются. Будет также полезно провести различие между возможными причинами подобного несоблюдения.

Некоторые возможные причины несоблюдения правил и процедур безопасности:

Непреднамеренные:

- Правозащитник не знает об этих правилах.
- Она/он не использует эти правила должным образом.

Преднамеренные:

Общие проблемы:

- Правила слишком сложные и их трудно соблюдать.
- Процедуры не очень доступны или представлены таким образом, что их трудно соблюдать в повседневной работе.

Индивидуальные проблемы:

- Правила противоречат индивидуальным потребностям и интересам, и это противоречие не разрешено.
- Человек не согласен с некоторыми или всеми правилами и считает их ненужными, неадекватными или неэффективными, основываясь на своем собственном опыте, либо в силу личных убеждений.

Групповые проблемы:

- Большинство членов организации, либо "лидеров", не соблюдают правил безопасности или соблюдают их не в полной мере вследствие отсутствия культуры безопасности в организации.
- Общее отсутствие мотивации на работе может привести к игнорированию правил безопасности.

Организационные проблемы:

- Отсутствие достаточных средств и технических возможностей, упрощающих соблюдение правил безопасности членами организации.
- Наличие противоречий между правилами безопасности и конкретной областью работы. Например, правила безопасности определены теми, кто несет за неё прямую ответственность, но они игнорируются или не выполняются соответствующим образом людьми, которые работают с программами или с отчетами. Некоторые правила могут соответствовать одной сфере деятельности и противоречить другой.
- Персонал имеет большую рабочую нагрузку и ограниченное время и не оценивает степени важности некоторых либо всех правил безопасности.
- Общее отсутствие мотивации, возникающее под воздействием стресса, споров на рабочем месте и т.д.

Культура организации носит как формальный, так и неформальный характер и должна развиваться не только в целом в организации, но и в отдельных её группах/командах. Хорошей культуре организации присущи такие признаки как неформальные беседы, шутки, вечеринки и т.д.

Мониторинг соблюдения правил и процедур безопасности

Прямой мониторинг:

Правила и процедуры безопасности могут быть включены в общие оценки работы и "контрольные списки" на совещаниях, проводимых до или после выездов на места событий, в рабочие отчеты, в повестки дня и т.д.

Периодически можно, вместе с проверяемой группой, проводить анализ таких вопросов, как хранение секретной информации, копий, руководств по безопасности, прравил посещения штаб-квартиры организации, подготовка к выезду на место событий и т.д.

Косвенный мониторинг:

Выяснение мнения людей о правилах и процедурах, об их соответствии и легкости их соблюдения и т.п., позволит установить, знаком ли персонал с этими правилами, принимаются ли эти правила полностью или имеется противоречие, которое необходимо устранить. Можно также проанализировать использование персоналом в своей работе данного Пособия по безопасности и любых других имеющихся протоколов и правил.

Очень полезно вместе с отдельными сотрудниками или контрольными группами собирать и анализировать мнения относительно правил и процедур безопасности. Это можно делать неформально/анонимно или с привлечением посредника.

Ретроспективный мониторинг:

Безопасность можно проверить путем анализа инцидентов, связанных с безопасностью, по мере их возникновения. Это следует делать особенно тщательно. Участник такого инцидента может быть обеспокоен тем, что это случилось по его вине и/либо тем, что такой анализ повлечет принятие против него санкций. Поэтому у неё/него может появиться соблазн скрыть этот инцидент и не сообщать о нем либо о некоторых его аспектах.

Кто проводит мониторинг?

В зависимости от того, как функционирует организация, мониторинг безопасности обычно проводят те люди, которые отвечают за безопасность организации или за конкретные участки работы по обеспечению безопасности и руководит персоналом безопасности.

Что можно сделать, если правила и процедуры безопасности не соблюдаются?

1 • Установить причины, найти решения и претворить их в жизнь. В качестве руководства можно также использовать перечень вариантов, приведенных в Таблице 1.

2 • Если проблема внутренняя и касается только одного сотрудника, попробуйте :

а • вступить в диалог с этим человеком и установить причину(ы) или мотив.

б • поговорите со всей группой, в которую он входит (иногда это неприемлемо, в зависимости от обстоятельств).

в • уведомите сотрудника заблаговременно, чтобы дать ему возможность должным образом осознать проблему.

г • используйте систему постепенных санкций, которая может в итоге привести к увольнению этого человека.

3 • Включите пункт о соблюдении правил и процедур безопасности во все рабочие контракты, чтобы весь персонал понимал, насколько это важно для организации.

Заключение,

Кое-кто может возразить, что обсуждение причин того, почему люди не соблюдают правила безопасности – это простая трата времени, так как существуют более неотложные и более важные проблемы, требующие незамедлительного решения. Те, кто разделяют это мнение, обычно считают, что правила надо соблюдать и точка. Другие считают, что в реальной жизни всё так просто.

Каким бы ни было ваше мнение, мы приглашаем вас оглянуться и проанализировать насколько правила и процедуры безопасности соблюдаются в той организации(-ях), в которой вы работаете. Результаты могут оказаться неожиданными, и над ними стоит задуматься с тем, чтобы избежать аналогичных проблем в будущем...

Повышение безопасности на работе и дома

Цель

Оценка безопасности на работе и дома.

Планирование, повышение и проверка безопасности в офисах и домах.

Безопасность на работе и дома

Безопасность в штаб-квартире или в офисах организации, а также в жилых домах членов семей сотрудников, исключительно важна для работы правозащитников. Поэтому далее мы подробно рассмотрим вопросы, связанные с анализом и повышением безопасности офиса или жилого помещения. (Для простоты мы будем называть их просто "офисы", хотя предлагаемая информация относится также к безопасности жилых помещений).

Общие аспекты безопасности офиса

Наши задачи по повышению безопасности можно свести к трем словам: **предотвратить несанкционированный доступ.** В редких случаях, необходимо также защитить офис от возможных нападений (например, от взрывов бомб).

Это подводит нас к первому общему рассуждению – уязвимые места офиса. Уязвимые места способствуют увеличению риска, в зависимости от стоящей перед вами угрозы. Например, если существует риск того, что кто-то украдет оборудование или информацию, то вы должны устранить эти уязвимые места соответствующим образом. Срабатывание сигнализации в ночное время принесет мало пользы, если никто не намерен идти и проверять, что произошло. С другой стороны, в случае грубого вторжения в дневное время, металлические решетки на дверях или сигнализация также не принесут особой пользы. Короче говоря, принимайте меры в соответствии со стоящей перед вами угрозой и в контексте вашей работы.

Уязвимые места офиса должны анализироваться в свете угроз, с которыми вы можете столкнуться.

Важно найти баланс между принятием необходимых мер безопасности и созданием у посторонних лиц впечатления, что что-то "прячется" или "охраняется", потому что это само по себе может поставить вас под угрозу. В организации безопасности офиса вам часто приходится выбирать между сдержанной позицией и принятием, в случае необходимости, более действенных мер.

Безопасность офиса оценивается по его наиболее уязвимому месту.

Если кто-то хочет попасть в офис без вашего ведома, то для этого он не будет искать самый сложный путь проникновения туда. Помните, что иногда самый простой способ проникновения в офис и получения информации о том, что там происходит – просто постучать в дверь и войти внутрь.

Место расположения офиса

При выборе места расположения офиса следует учитывать следующие факторы: местоположение; связано ли выбираемое здание с какими-либо конкретными людьми либо с прошедшими событиями; близость к общественному и частному транспорту, риск несчастных случаев; насколько помещение удобно для проведения мер безопасности и т.д. (см. также раздел Оценка риска расположения ниже).

Полезно также провести анализ того, какие меры безопасности принимаются другими лицами в этом районе. Большой объем мер безопасности может быть признаком того, что этот район небезопасен, например, в связи с высоким уровнем преступности в нём. Важно также поговорить с местными жителями о состоянии безопасности в этом районе. В любом случае, постарайтесь, чтобы принимаемые меры безопасности не привлекали ненужного внимания. Полезно также познакомиться с местными жителями, так как они могут дать вам полезную информацию обо всем подозрительном, происходящем поблизости.

Важно также проверить, кто является вашим домовладельцем. Какой репутацией он пользуется? Насколько он может быть чувствителен к давлению властей? Будет ли он возражать против установки в помещении средств безопасности?

При выборе офиса необходимо учитывать и то, кто именно будет приходить в него. К офису, куда приходят пострадавшие в поисках юридических консультаций, предъявляются иные требования, чем к офису, который, главным образом, является местом работы персонала. Важно учитывать близость маршрутов общественного транспорта, насколько этот факт может повлиять на безопасность проезда персонала от места проживания к месту, где осуществляется основная деятельность организации, и т.д. Необходимо провести оценку прилегающих районов, в частности, для того, чтобы избежать проезда через небезопасные зоны.

После выбора места расположения офиса, важно периодически проводить оценку аспектов выбора, которые могут изменяться, например, в случае поселения поблизости "нежелательного элемента".

КОНТРОЛЬНАЯ ТАБЛИЦА ВОПРОСОВ ДЛЯ ВЫБОРА БЛАГОПРЯТНОГО РАСПОЛОЖЕНИЯ ОФИСА	
Ближайшее окружение:	Статистика преступлений; близость к потенциальным объектам вооруженного нападения, таким как военные или правительственные учреждения; безопасные места для приема беженцев; близость к прочим национальным и международным организациям, с которыми вы поддерживаете отношения.
Взаимоотношения:	Тип проживающих по соседству людей; владелец/домовладелец, бывшие жильцы помещений; предыдущие виды использования здания.
Доступность:	Наличие одного или нескольких хороших маршрутов подъезда (чем больше, тем лучше); удобство подъезда общественным или частным транспортом.
Уличное освещение	Наличие воды, электричества, телефона.
Основные коммунальные службы	На окружающей территории.
Подверженность несчастным случаям или естественным рискам:	Пожары, значительные наводнения, оползни, сброс опасных материалов, промышленные предприятия с опасными технологическими процессами и т.д.
Физическое состояние здания:	Прочность сооружения, возможности установки специального оборудования, наличие дверей и окон, ограждения по периметру и защитных барьеров, точек входа (см. ниже).
Условия для транспорта:	Наличие гаража, небольшого двора или закрытого участка с парковочным барьером.

Доступ третьих лиц к офису: Физические барьеры и процедура приема посетителей

Теперь вы знаете, что основная цель безопасности офиса – предупреждение несанкционированного доступа туда людей. Человек или группа людей могут проникнуть на территорию офиса с целью совершения кражи, получения информации; с целью подбросить туда что-нибудь с тем, чтобы использовать это против вас в дальнейшем, например, наркотики, оружие; для передачи угроз и т.д. Каждый случай индивидуален, но ваша цель остается неизменной – избежать его.

Доступ в здание контролируется с помощью **физических барьеров** (заборов, дверей, ворот), с помощью **технических средств** (таких как сигнализация) и **процедуры приема посетителей.** Любой барьер (и любая процедура) представляет собой **фильтр**, через который должен пройти каждый, кто хочет попасть в офис. В идеале, для создания нескольких рядов защиты эти фильтры должны быть комбинированными, способными предотвратить различные виды несанкционированного входа в офис.

Физические заграждения

Заграждения предназначены для **физической** блокировки входа посторонних. Эффективность физических преград зависит от их **надежности** и способности блокировать проход через все **уязвимые места** в стенах.

Ваш офис может иметь физические заграждения в трех зонах:

1 • **Внешний** периметр: заборы, стены или нечто подобное за пределами сада или двора.

2 • Периметр **здания или помещений.**

3 • **Внутренний** периметр: Барьеры, которые могут быть созданы в пределах самого офиса для защиты одной или нескольких комнат. Это особенно полезно для офисов с большим количеством посетителей, поскольку это позволяет отделить общую зону от более закрытой зоны, которая может быть защищена дополнительными заграждениями.

Внешний периметр

Офис должен быть окружен четким внешним барьером, скажем, высоким или низким забором, желательно прочным и высоким, чтобы затруднить проникновение. Металлическая ограда или решетка позволят вести наблюдение за деятельностью организации, поэтому лучше если стены будут сплошными - из кирпича или аналогичного материала.

Периметр здания или помещения

Он включает стены, двери, окна, потолок или крышу. Если стены прочные, то все проемы и крыша также будут прочными. Двери и окна должны иметь соответствующие запоры и должны быть усилены решетками, желательно с вертикальными и горизонтальными прутьями, хорошо вмонтированными в стены. Крыша также должна иметь хорошую защиту, а не просто слой оцинкованного железа или черепицы. Если усилить крышу невозможно, заблокируйте все доступы к ней с земли или со стороны примыкающих зданий.

В местах, сопряженных с риском вооруженного нападения, важно создать зоны безопасности в пределах самого офиса (см. Главу 11 о безопасности в зонах вооруженных конфликтов).

Внутренний периметр

Сказанное выше также справедливо и в отношении внутренних помещений. Очень полезно иметь зону с дополнительными средствами безопасности внутри офиса; как правило, организация такой зоны довольно проста. Даже сейф можно рассматривать как один из элементов периметра внутренней безопасности.

Несколько слов о ключах

- Ключи не должны находиться в поле зрения или досягаемости посетителей. Храните все ключи в шкафу или в ящике с простой комбинацией замка, код которого известен только штатным сотрудникам. Для большей безопасности код должен периодически меняться.

- Если ключи имеют индивидуальные бирки, не помечайте их надписями, указывающими на определенную комнату, шкаф или ящик, так как это упростит ограбление. Используйте для этого нумерацию, буквенное обозначение или цветовое кодирование.

Технические меры: Освещение и сигнализация

Технические средства дополняют физические преграды либо процедуры приема посетителей. К ним относятся дверные глазки, системы двусторонней связи и видеокамеры (см. ниже). Это происходит оттого, что **технические средства эффективны лишь тогда, когда они нацелены на предотвращение вторжений.** Эффективные технические средства призваны вызывать определенную реакцию, например, привлекать внимание соседей, полиции или частного охранного агентства. Если этого не происходит, и нарушитель знает, что никакой реакции не последует, то такие меры малоэффективны и сводятся лишь к предупреждению мелких краж или регистрации входящих людей.

- **Освещение** вокруг здания (дворов, садов, тротуаров), а также его лестничных площадок, очень важно.
- **Сигнализация** преследует несколько целей, включая обнаружение незаконно проникших лиц, предотвращение потенциального вторжения или пресечение попыток вторжения.

Сигнализация может привести в действие звуковой сигнал внутри офиса; световую сигнализацию; общий звуковой сигнал, звонок или иной звуковой эффект; либо сигнал в центр защиты извне. Звуковой сигнал эффективен для привлечения внимания, но он может иметь и обратный эффект при возникновении конфликтной ситуации или в тех случаях, когда вы не предполагаете, что местные жители либо прохожие могут отреагировать на него. Необходим очень взвешенный выбор между звуковой и световой сигнализацией (сильный постоянный свет или мигающий красный свет). Последний может быть достаточным для сдерживания нарушителя, так как он предполагает, что после обнаружения вторжения последуют дополнительные действия.

Сигнализация должна устанавливаться в точках входа (во дворах, на дверях, окнах и других охраняемых помещениях, таких как помещения, где хранится важная информация). Наиболее эффективна сигнализация с датчиками-фотоэлементами, которые при обнаружении движения активизируют световой или звуковой сигнал или видеокамеру.

Сигнализация должна:

- иметь аккумуляторную **батарею**, чтобы работать и при отключении электричества.
- срабатывать с **задержкой по времени**, чтобы персонал имел возможность отключить её в случае ошибочного приведения ее в действие.
- иметь, в случае необходимости, возможность **ручного** включения.
- легко **устанавливаться** и **демонтироваться**.
- легко отличаться от пожарной сигнализации.

Видеокамеры

Видеокамеры могут способствовать улучшению процедур пропуска (см. ниже) или учета людей, приходящих в офис. В то же время, видеозапись должна вестись с точки, недоступной для нарушителей. В противном случае, они могут взломать видеокамеру и уничтожить пленку.

Возможно, вам придется подумать над тем, будут ли камеры отпугивать людей, которых вы ждете, таких как пострадавшие или свидетели, или они будут расцениваться как ценности и привлекать внимание воров. Опыт подсказывает, что в случае использования камер наблюдения, полезно разместить рядом с ними соответствующие письменные предупреждения (право на частную жизнь также относится к правам человека).

Частные охранные компании

Этот вопрос требует большой осторожности. Во многих странах частные охранные компании укомплектованы бывшими сотрудниками сил безопасности. Имеются документально подтвержденные случаи, когда такие люди привлекались к ведению наблюдения и нападению на правозащитников. Поэтому целесообразно не доверять охранным компаниям, если у вас есть основания опасаться слежки или нападения со стороны сил безопасности. Если охранная компания имеет доступ к вашему офису, она может установить микрофоны или позволить проникновение туда других людей.

Если вы считаете, что вам необходимо использовать охранную компанию, вы должны убедиться, что у вас есть чёткое соглашение о том, что именно разрешено её сотрудникам, а также о том, какие действия вами запрещены и в какие именно части здания они имеют право входить. Безусловно, вы также должны иметь возможность контролировать соблюдение условий договора.

Например:

> Если вы наняли службу охраны, которая, в случае срабатывания сигнализации, высылает охранника, этот охранник может иметь доступ к уязвимым местам вашего офиса и установить подслушивающие устройства в вашем зале заседаний.

Лучше договориться о том, кто конкретно будет на вас работать (и при возможности провести проверку этих лиц), но это редко осуществимо.

Если охранники имеют при себе оружие, то для организации по защите прав человека важно иметь четкое представление о том, в каких случаях они будут уполномочены его применить. Но ещё более важно сопоставить потенциальные преимущества и отрицательные стороны применения ими оружия. Лёгкое огнестрельное оружие не является сдерживающим фактором в случае нападения с применением оружия с большей огневой мощью (как это обычно и происходит), но если нападающие знают, что в вашем офисе имеются легковооруженные охранники, то они могут вторгнуться туда с готовностью открыть огонь для собственной защиты. Другими словами, некоторая боеготовность (легкое оружие) может, вероятно, спровоцировать нападающих на открытое применение оружия с большей мощностью поражения. Наступает момент, когда стоит спросить себя, нужны ли вам охранники с автоматами и даёт ли это вам достаточное социо-политическое пространство для выполнения своей работы?

Фильтры процедуры допуска

Физические барьеры должны дополняться "фильтром" **процедуры допуска**. Эти процедуры определяют когда, как и кто имеет право входа в любую часть офиса. Допуск к уязвимым местам, где хранятся ключи, информация и деньги, должен быть ограничен.

Самый простой способ входа в офис, в котором работают правозащитники – постучаться в дверь и войти. Многие люди делают это каждый день. Чтобы уравновесить открытый характер офиса правозащитников с необходимостью контроля посетителей и целью их прихода, вам необходима соответствующая процедура пропуска.

Как правило, у людей есть конкретные причины, для того чтобы постучать в вашу дверь либо войти внутрь офиса. Часто люди хотят задать вопрос или что-нибудь сообщить, не спрашивая на это разрешения. Давайте проанализируем эту проблему поэтапно:

Кто-то звонит и спрашивает разрешения войти по какому-то конкретному вопросу

В этом случае вам следует выполнить три простых шага:

1 • **Спросите, почему этот человек хочет войти.** Если она/он хочет встретиться с одним из сотрудников офиса, спросите об этом у сотрудника. Если этот сотрудник отсутствует, попросите посетителя прийти в другое время или подождать где-нибудь за пределами запретной зоны. Важно пользоваться дверными глазками, видеокамерами или переговорными телефонами на входе в офис, чтобы не приближаться к двери и не открывать её, особенно если вы не хотите впустить кого-либо внутрь или столкнуться с угрозой насильственного или грубого вторжения. Поэтому желательно иметь зону ожидания, которая физически отделена от внутреннего входа в офис. Если есть необходимость в организации легкодоступной для посетителей зоны, обеспечьте физические барьеры, блокирующие доступ к остальным зонам офиса, куда вход ограничен.

Кто-то может попросить войти в офис с целью проверки или ремонта водопровода или электросетей, или для выполнения другого ремонта. Она/он может также утверждать, что является представителем каких-либо средств массовой информации, официальных властей и т.д. Перед тем как их впустить, получите подтверждение их личности у компании или организации, представителем которой они назвались. Помните, ни специальная униформа, ни удостоверение личности не являются достаточной гарантией безопасной идентификации, особенно в ситуациях со средним и высоким уровнем риска.

2 • **Решите, разрешить или не разрешить вход.** После установления цели визита, вам предстоит решить, разрешить или не разрешить вход. Ответ на вопрос о цели визита ещё не служит достаточным основанием для того, чтобы впустить постороннего. Если вы не уверены, с какой миссией она/он прибыли, не давайте разрешение на вход.

3 • **Наблюдайте за посетителями, пока они не уйдут.** После входа посетителя в офис убедитесь, что кто-то из сотрудников постоянно сопровождает его до момента выхода из офиса. Для приема посетителей целесообразно иметь отдельное помещение в стороне от комнат с ограниченным доступом.

Необходимо вести регистрацию всех посетителей с указанием их фамилий, организаций, цели визита, с кем они встречались, когда прибыли и когда ушли. Это может оказаться чрезвычайно важным для анализа причин инцидента, связанного с безопасностью.

Кто-то приезжает или звонит по какому-либо вопросу

Независимо от того, что может сказать звонивший или посетитель, вы ни при каких обстоятельствах не должны сообщать им местонахождение коллеги или других людей либо давать ему информацию личного характера. В случае настойчивости спрашивающего, попросите его оставить сообщение, перезвонить или прийти позже, либо договориться о встрече заблаговременно.

Иногда люди приходят по ошибке и спрашивают, проживает ли здесь такой-то или продается ли здесь что-либо и т.д. Некоторые хотят что-то продать, нищие могут приходить с просьбами о помощи. Если вы откажетесь впустить этих людей или сообщить им какую-либо информацию, вы избежите риска для вашей безопасности.

Кто-то хочет передать предмет или сверток

Риск, которому вы себя подвергаете при получении какого-либо предмета, пакета или свертка, состоит в том, что их содержимое может скомпрометировать вас или причинить вам ущерб, особенно, если там бомба. Неважно, какими невинными они могут казаться, не прикасайтесь к ним и не разворачивайте их до тех пор, пока вы не выполнили три следующих шага:

1 • **Проверьте, ожидает ли предполагаемый получатель этот пакет.** То, что получатель знает отправителя, ещё недостаточно, так как личность отправителя можно легко сфальсифицировать. Если получатель, для которого предназначен этот пакет, не ждет его, он должен проверить, действительно ли предполагаемый отправитель прислал ему этот пакет. Если пакет направлен просто в адрес офиса, проверьте, кто его отправил. Подождите и обсудите этот вопрос, прежде чем принять окончательное решение.

2 • **Решите, принимать или не принимать пакет или письмо.** Если вы не можете установить отправителя или на это потребуется время, то лучше всего не принимать пакет, особенно в условиях среды с высокой степенью риска. Вы всегда можете попросить передать его позже или забрать его в почтовом отделении.

3 • **Проследите перемещение пакета внутри офиса.** Убедитесь в том, что вы знаете, в каком месте офиса он находится до передачи получателю.

При выполнении функциональных обязанностей и на приемах

В этих условиях правила просты: не позволяйте входить лицам, которых вы и ваши коллеги не знаете лично. Пропускать следует только тех людей, которые известны вам или вашему коллеге, которому вы доверяете, и только при условии, что этот коллега присутствует и может подтвердить личность визитёра. Если кто-то из прибывших говорит, что он знает кого-то в офисе, а этого человека нет на месте, не впускайте его.

Ведение регистрации телефонных звонков и посетителей

Целесообразно вести регистрацию телефонных звонков и номеров телефонов, а также регистрацию посетителей офиса (в некоторых организациях новых посетителей просят предъявить документ, подтверждающий их личность, и регистрируют номер документа).

Сверхурочная работа в офисе

Для сверхурочной работы персонала должна быть разработана специальная процедура. Члены организации, планирующие остаться для выполнения сверхурочной работы в вечернее и ночное время, должны до определенного часа уведомить об этом специально назначенного для этого сотрудника организации и принять особые меры предосторожности при уходе из офиса и т.д.

КОНТРОЛЬНАЯ ТАБЛИЦА ВОПРОСОВ: ОПРЕДЕЛЕНИЕ УЯЗВИМЫХ МЕСТ В ПРОПУСКНОЙ СИСТЕМЕ
• **Кто** имеет постоянный доступ, **к каким** зонам и **почему**?
• Разделите всех посетителей **по типам** (курьеры, обслуживающий персонал, специалисты-компьютерщики, члены НПО, приезжающие на совещания , высокопоставленные лица, гости, приезжающие по служебным делам и т.д.) и **разработайте соответствующие правила пропуска для каждого** из них. Весь персонал должен быть ознакомлен со правилами приема всех типов посетителей и нести ответственность за их соблюдение.
• Если посетитель вошёл в офис, имеет ли он доступ к уязвимым местам? Разработайте стратегии для предупреждения этого.
КОНТРОЛЬНАЯ ТАБЛИЦА: ДОСТУП К КЛЮЧАМ
• **Кто** имеет доступ, **к каким** ключам и **когда**?
• Где и как **хранятся ключи** и **дубликаты** этих ключей?
• Ведется ли учет дубликатов ключей, находящихся в обращении?
• Есть ли риск того, что кто-то изготовит **дубликат ключа без разрешения**?
• Что произойдет, **если утерян ключ**? Соответствующий замок должен быть заменен, кроме тех случаев, когда вы абсолютно уверены в том, что ключ утерян случайно, и никто не сможет установить его владельца или ваш адрес. Помните, что ключ могут выкрасть, например, путем инсценировки грабежа, для того, чтобы кто-то мог проникнуть в ваш офис.

Все члены организации несут ответственность за принятие мер против любого человека, не соблюдающего правил пропуска. Кроме того, в журнале учета инцидентов, связанных с безопасностью, они должны вести регистрацию всех передвижений подозрительных лиц либо автомобилей. То же самое относится и к любому предмету, оставленному вне офиса, чтобы исключить риск возможной установки бомбы. Если вы подозреваете последнее, не игнорируйте подозрительный предмет, **не прикасайтесь к нему** и вызовите полицию.

При переезде в новый офис или если ключи утеряны или украдены, очень важно сразу же сменить все дверные замки.

Проверочный список: Основные процедуры безопасности офиса

- ☐ Установите огнетушители и сигнальное освещение (со сменяемыми батареями). Убедитесь, что весь персонал знает, как ими пользоваться.
- ☐ Установите электрогенератор, если вероятность отключений электроэнергии высока. Отключения электроэнергии могут поставить под угрозу систему безопасности (систему освещения, сигнализации, телефонов и т.д.), особенно в сельских районах.
- ☐ Храните под рукой список экстренных номеров телефонов: полиции, пожарной части, скорой помощи, ближайшей больницы и т.д.

- При наличии риска конфликта в непосредственной к вам близости, обеспечьте запасы продовольствия и воды.

- Определите местонахождение безопасных зон за пределами офиса на случай экстренной необходимости (например, офисы других организаций).

- Не оставляйте посторонних лиц **одних** в уязвимых зонах с доступом к ключам, информации или ценным вещам.

- **Ключи:** Никогда не оставляйте ключи в местах, к которым посетители могут иметь доступ. Никогда не "прячьте" ключи у входа в офис – это делает их доступными для посторонних.

- **Правила пропуска:** Барьеры безопасности не обеспечат защиту, если потенциальный злоумышленник пропущен в офис. Здесь важно помнить следующее:

  - Весь персонал несет ответственность за контроль посетителей и их пропуском.

  - Все посетители должны сопровождаться во время всего посещения офиса.

- При обнаружении посетителя, незаконно проникшего в офис:

  - Никогда не вступайте в конфликт с человеком, готовым к применению насилия для достижения своей цели (например, если он вооружен). В таких случаях, подайте сигнал опасности коллегам, найдите безопасное место для укрытия и попросите помощи у полиции.

  - Осторожно приблизьтесь к этому человеку или воспользуйтесь помощью коллег либо полиции.

- В ситуациях с высокой степенью риска всегда держите под контролем уязвимые места, такие как, например, информация, сохраняемая на жестком диске компьютера, с тем, чтобы сделать их недоступными или уничтожить в случае экстренной эвакуации.

- Помните, что в случае конфронтации с потенциальным злоумышленником, люди, работающие в офисе, находятся как бы на переднем крае. Убедитесь, что они достаточно подготовлены и обладают необходимой поддержкой в любой ситуации, при этом не навлекая на себя риска.

Регулярные проверки безопасности офиса

Регулярные проверки или инспекции безопасности офиса очень важны, так как с течением времени ситуации и правила изменяются, например, в связи с устареванием оборудования или в связи с большой текучестью кадров. Важно также обновлять своё представление о степени владения персоналом правилами безопасности офиса.

Лицо, отвечающее за безопасность, должно проводить не менее одной проверки безопасности офиса **каждые шесть месяцев**. С помощью представленного ниже контрольного вопросника, эта проверка займет немного времени, не более одного-двух часов. Лицо, отвечающее за безопасность, перед составлением окончательного отчета должно обеспечить обратную связь с персоналом и затем представить организации отчет для принятия необходимых решений и действий. После этого, отчет должен храниться в архивах до проведения очередной проверки безопасности.

КОНТРОЛЬНАЯ ТАБЛИЦА ВОПРОСОВ: ПРОВЕРКА БЕЗОПАСНОСТИ ОФИСА

Вид проверки:
Выполнил:
Дата:

1 • КОНТАКТЫ В КРИТИЧЕСКИХ СИТУАЦИЯХ:

- Имеется ли под рукой список обновленных телефонов и адресов других НПО, больниц неотложной помощи, полиции, пожарной части и скорой помощи?

2 • ТЕХНИЧЕСКИЕ И ФИЗИЧЕСКИЕ БАРЬЕРЫ (ВНЕШНИЕ, ВНУТРЕННИЕ И ВНУТРИ ОФИСА):

- Проверьте состояние и исправность ворот/заборов, дверей ведущих в здание, окон, стен и крыши.
- Проверьте состояние и исправность внешнего освещения, сигнализации, видеокамер и видеотелефонов на входе.
- Проверьте правила выдачи ключей, включая ключей, которые находятся под охраной и имеющих кодировку, распределение обязанностей по контролю за ключами и их дубликатами. Ключи и их дубликаты должны быть в исправном состоянии. В случае утери или кражи ключей, обеспечьте смену замков и регистрацию этих инцидентов.

3 • ПРАВИЛА ПРОПУСКА ПОСЕТИТЕЛЕЙ И "ФИЛЬТРЫ":

- Распространяются ли правила пропуска на все категории посетителей? Все ли сотрудники ознакомлены с ними?
- Проанализируйте все инциденты, связанные с безопасностью и имеющие отношение к правилам пропуска посетителей или "фильтрам".
- Опросите сотрудников, обычно занимающихся пропуском посетителей, насколько эффективны правила пропуска и что требуется для их улучшения.

4 • БЕЗОПАСНОСТЬ В СЛУЧАЕ ВОЗНИКНОВЕНИЯ ИНЦИДЕНТОВ:

- Проверьте состояние огнетушителей, газовых вентилей/ трубопроводов, водопроводных кранов, электрических предохранителей и электрогенераторов (если таковые имеются).

5 • РАСПРЕДЕЛЕНИЕ ОБЯЗАННОСТЕЙ И ОБУЧЕНИЕ:

- Распределены ли обязанности по обеспечению безопасности офиса? Эффективны ли они ?
- Имеется ли программа подготовки по обеспечению безопасности офиса? Охватывает ли она все сферы подготовки, упомянутые в настоящем анализе? Все ли новые члены организации прошли подготовку? Эффективна ли эта подготовка?

Безопасность и женщины-правозащитницы

Цель

Анализ специальных мер по безопасности женщин-правозащитниц.

Ниже приведены некоторые основные вопросы, связанные с безопасностью женщин-правозащитниц. Эта тема требует более глубокого анализа, основанного на практическом опыте женщин-правозащитниц. Более подробная информация на эту тему будет представлена в материалах Международного Совещания по вопросам женщин-правозащитниц в 2005 году.

Женщины-правозащитницы

Женщины всегда играли важную роль в расширении и защите прав человека, однако, их роль не всегда воспринималась положительно. В деле защиты прав человека женщины работают как независимо, так и вместе с мужчинами[1]. Многие женщины входят в состав организаций, работающих от имени пропавших без вести людей и заключенных. Одни из них защищают права национальных меньшинств или жертв сексуального насилия, другие являются членами профсоюзов, юристами и участницами правозащитных кампаний.

Нападения на женщин-правозащитниц

В своем **ежегодном отчете за 2002 год, представленном Комиссии по правам человека,** Хина Джилани, специальный представитель ООН по делам правозащитников, отмечает:

> Женщины-правозащитницы, наравне со своими коллегами-мужчинами, действуют на передовой линии борьбы за соблюдение и защиту прав человека. При этом, будучи женщинами, помимо риска с которым сталкиваются мужчины, они сталкиваются с риском, характерным для их пола.

[1] Очень полезное руководство для женщин-правозащитниц можно найти на веб-сайте Управления Верховного комиссара по делам беженцев (УВКБ) http://www.unhchr.ch/defenders/tiwomen.htm. Также см. доклад: Совещание по вопросам женщин-правозащитниц со специальным представителем Генерального секретаря ООН, 4-6 апреля 2003 г., опубликованного «Asia Pacific Forum on Women, Law and Development» и «Essential actors of our time. Human rights defenders in the Americas», опубликованного «Эмнисти Интернэшнл».

Во-первых, как женщины они более заметны. То есть, женщины-правозащитницы могут вызвать большую враждебность, чем их коллеги-мужчины, так как, будучи женщинами, они могут тем самым противоречить некоторым культурным, религиозным или социальным нормам в отдельных странах и регионах. В этом контексте, как женщины-правозащитницы они могут столкнуться не только с нарушением прав человека, но и с другим риском, связанным с их полом, поскольку их работа может приходить в противоречие с социальными стереотипами о женщине, её покорном характере или бросать вызов устоявшимся в обществе понятиям о статусе женщины.

Во-вторых, нельзя исключать, что враждебность, сексуальные домогательства и притеснение женщин-правозащитниц могут принять особую форму, основанную на половом признаке, начиная, например, от устного оскорбления, направленного исключительно против женщины, и заканчивая изнасилованием.

В этой связи, профессиональная честность женщин и их положение в обществе могут быть поставлены под угрозу и дискредитированы такими специфичными способами, как публично высказываемые сомнения в их неподкупности, особенно в тех случаях, когда женщины заявляют о своем праве на сексуальное и репродуктивное здоровье или на равное с мужчинами право на жизнь, свободную от дискриминации и насилия. В этом контексте, например, женщины-правозащитницы борются с законами, ставящими под сомнение правомерность их поведения, направленного на равное пользование правами, защищенными международным законом, против ложных обвинений, выдвинутых против них по причине их взглядов и деятельности в защиту прав женщин.

В третьих, нарушения прав человека, совершенные против женщин-правозащитниц, могут, в свою очередь, вызвать ответные действия, которые сами по себе имеют половую направленность. Например, сексуальное оскорбление женщины-правозащитницы при задержании и её изнасилование могут привести к беременности и к заражению сексуально венерическими болезнями, включая ВИЧ/СПИД.

Некоторые специфически женские права поддерживаются и защищаются исключительно женщинами-правозащитницами. Поддержка и защита женских прав может быть дополнительным фактором риска, так как утверждение некоторых этих прав рассматривается кое-где как угроза патриархальному укладу жизни и как подрыв культуры, религии и общественной морали. Защита права женщин на жизнь и свободу в некоторых странах поставила под угрозу жизнь и свободу самих женщин-правозащитниц. Точно так же, протесты против дискриминационной практики привели к преследованию выдающихся мужчин, борющихся за права женщин, под предлогом обвинения их в «отступничестве».

Необходимо также учитывать такие факторы как возраст, этническое происхождение, образование, сексуальная ориентация и семейное положение, так как различные группы женщин-правозащитниц сталкиваются с разными проблемами, и поэтому у них разные потребности в безопасности и защите.

Оценка проблем защиты женщин-правозащитниц позволит определить специфические и часто различные потребности и уязвимые места и воспользоваться эффективными уже существующими стратегиями женщин-правозащитниц. Таким образом, это позволит более адекватно решать проблемы, возникающие в критических ситуациях и в повседневной жизни.

Безопасность женщин-правозащитниц

Женщины-правозащитницы платят высокую цену за свою работу по защите и содействию соблюдения прав других людей. Они сталкиваются с риском, характерным только для их пола, поэтому их безопасность требует специального подхода. Для этого имеются следующие причины:

Женщины могут привлекать нежелательное внимание.

Женщины-правозащитницы могут спровоцировать враждебное отношение, связанное с тем, что они - женщины и одновременно правозащитницы, способные бросить вызов местным культурным и религиозным традициям и социальным нормам, сложившимся в отношении женщин и их роли в обществе. Поэтому женщины-правозащитницы могут столкнуться с нарушением прав человека не только в силу своей работы, но и по причине того, что они являются работающими женщинами, или могут бросить вызов устоявшимся стереотипам о покорном женском характере и ложным представлениям о её статусе.

Женщины-правозащитницы могут быть вынуждены нарушить определенные законы и социальные табу.

В некоторых странах защита прав женщин на жизнь и свободу привела к нарушению прав самих женщин-правозащитниц. Точно так же, протесты против дискриминационной практики привели к преследованию выдающихся мужчин, борющихся за права женщин, под предлогом их обвинения в «отступничестве». Во многих культурах требование подчинения женщины мужчине в общественной жизни может служить препятствием в тех случаях, когда женщины публично занимаются расследованием нарушений прав человека, совершенных мужчинами. Определенная дискриминационная или сексуально-ориентированная интерпретация религиозных текстов также часто используется для сохранения или принятия законов или практики, имеющих огромное влияние на права женщин.

Специальные виды агрессии против женщин-правозащитниц.

Враждебность, сексуальные домогательства и давление, с которыми могут столкнуться женщины-правозащитницы, могут принимать особую форму, основанную на половом признаке, начиная, например, от устного оскорбления, направленного исключительно против женщины, и заканчивая изнасилованием. Последствия такой агрессии также могут быть специфичными только для женщин (например, беременность либо социальная отверженность).

Женщины-правозащитницы могут оказаться в положении, требующем "доказательств" их честности:

Женский профессионализм и положение в обществе могут оказаться под угрозой или дискредитироваться специфичными для них способами, например, постановкой под сомнение их честности.

Коллеги-мужчины могут не понимать или даже отвергать работу женщин-правозащитниц:

Коллеги-мужчины могут иметь такие же социальные предрассудки, как и посторонние люди, совершающие нападения на женщин-правозащитниц. Кроме того, мужчины могут быть обеспокоены профессиональной компетентностью женщин. Всё это может привести к попыткам ограничить или торпедировать работу женщин-правозащитниц, что иногда заканчивается сексуальными домогательствами и насилием против женщин-правозащитниц, совершаемым их коллегами-мужчинами.

Женщины-правозащитницы могут подвергаться насилию в быту:

Насилие в быту может возникнуть в связи с изменением структуры власти в семье. Растущая профессиональная роль женщины-правозащитницы и её влияние могут привести к тому, что её муж, сожитель или другие члены семьи видят в этом угрозу для себя и стремятся прекратить её правозащитную деятельность либо совершают насилие. Бытовое насилие против женщины включает все виды физического, сексуального и психологического насилия, совершаемого в семье, такие как побои, супружеское изнасилование, нанесение сексуальных увечий и другие традиционные практики, наносящие вред женщине (см. ниже).

Дополнительные семейные обязательства:

Помимо своей работы, многие женщины-правозащитницы должны заботиться о детях и других членах своих семей. Эти обязательства, особенно связанные с маленькими детьми, могут оказывать влияние на принятие мер, связанных с безопасностью женщины-правозащитницы, в ситуациях с высокой степенью риска.

Повышение безопасности женщин-правозащитниц

Важно признать, что женщины-правозащитницы представляют собой широкий спектр индивидуальностей, сталкивающихся с различными проблемами, имеющих различный опыт и нуждающихся в различных решениях стоящих перед ними проблем. Самое важное помнить, что в любой конкретной ситуации, связанной с безопасностью, женщины являются прежде всего правозащитницами, способными выявить проблемы и найти способы их решения. Для этого необходим анализ как вопросов расширения сфер работы женщин-правозащитниц, так и вопросов обеспечения специфических для них условий безопасности и организации их обучения:

Расширение сфер работы женщин

В сжатом виде, это означает обеспечение полного участия женщин наряду с мужчинами в принятии решений, включение вопросов безопасности женщин в повестки дня совещаний и равное с мужчинами участие женщин в процессе принятия мер безопасности. Важно учитывать их опыт в формировании правил и процедур безопасности, а также в их оценке и мониторинге.

Обеспечение специфичной для женщин безопасности и защиты

Как и в других случаях обеспечения безопасности, распределение обязанностей для принятия мер, направленных против специфического для женщин-правозащитниц риска насилия, очень важно в организации или группе правозащитников. В идеале, лица, отвечающие за безопасность, должны иметь хорошее понимание специфики проблем, связанных с безопасностью женщин-правозащитниц. Иногда для этого необходимы новые люди, способные привнести специальные знания и представления по данному вопросу. Например, кто-то отвечает за безопасность, но через некоторое время организация принимает решение назначить другого человека, имеющего подготовку и навыки, более подходящие для защиты от специфического для женщин-правозащитниц насилия. В таких случаях, сотрудничество должно быть более тесным, чтобы обеспечить надежное функционирование всех мер безопасности и реагирование на различные проблемы.

Обучение

Обучение всех сотрудников правозащитной организации является ключевым моментом в повышении безопасности и защиты и должно включать развитие навыков осознания проблем, специфических для женщин-правозащитниц.

Количество случаев насилия, связанного с половой принадлежностью, всегда **занижается.** Общее в организации или группе представление о насилии, связанном с половой принадлежностью, упрощает обсуждение проблем, связанных с угрозами или инцидентами, в основе которых лежит половой признак.

Желающие члены организации могут взять на себя функции «посредников» между женщинами и мужчинами-правозащитниками, которые хотят решить проблемы, связанные с угрозой или насилием, в основе которых лежит половой признак, совершенными в отношении их самих или в отношении других членов организации, группы или общины.

Резюме,

Отличие проблем, связанных с женской безопасностью состоит в ином характере угроз и в различиях между ситуациями (такими как задержание, работа на месте событий и т.д.). Цель состоит в том, чтобы разработать меры, учитывающие половую принадлежность, для предупреждения насилия над женщинами и другими правозащитниками.

Сексуальные нападения и личная безопасность

Предупреждение сексуальных нападений может быть аналогичным предупреждению других видов агрессии, особенно тех, которые связаны с обычными преступлениями. Сексуальные нападения могут принимать форму давления на работу правозащитника, причем жертва может быть выбрана заранее или конъюнктурно.

Все – мужчины и женщины – являются потенциальными жертвами сексуального нападения, но женщины чаще служат мишенью таких нападений. Сексуальное нападение – это преступление с позиции **власти** и насилия, а сексуальный контакт для нападающего - всего лишь один из способов демонстрации своей власти над жертвой.

Помните, что во многих случаях изнасилованию (а также избиению и даже смерти) подвергаются женщины, которые выезжают в другие районы вместе с потенциальным злоумышленником. Таким образом, женщины всегда должны принимать жесткое и однозначное решение не выезжать в другие районы с потенциальным насильником (возможно, за исключением тех случаев, когда отказ представляет серьезную угрозу для её жизни или для жизни других людей).

Реакция на сексуальное нападение[2]

Выбор варианта реакции на сексуальное нападение ограничен и принимает его только сама жертва насилия. Не существует правильного или неправильного способа реагирования. В любом случае, главная цель – выжить. Выбор, имеющийся в распоряжении жертвы сексуального нападения, может включать следующее:

1 • **Покорность:** Если жертва опасается за свою жизнь, она должна подчиниться преступнику.

2 • **Пассивное сопротивление:** Сделайте или скажите что-нибудь неприятное либо вызывающее отвращение, чтобы разрушить у насильника желание к сексуальному контакту. Скажите ему, что у вас СПИД, понос, заставьте себя вырвать и т.д.

3 • **Активное сопротивление:** Попробуйте применить любую физическую силу на которую вы способны, чтобы отбить нападение, например, вы можете бить преступника руками и ногами, кусаться, царапаться, кричать или спасаться бегством.

Во всех случаях делайте всё, чтобы выжить. Следуйте своим инстинктам. Никто не знает, как он будет реагировать в такой ситуации и ваша реакция будет единственно правильной для вас.

После совершения сексуального нападения

Все организации и группы правозащитников должны иметь готовые планы предупреждения и реагирования на инциденты, связанные с сексуальными нападениями. План реагирования должен включать, как минимум, предоставление жертве насилия **эффективной медицинской помощи, включая психологическую** (проверить сразу и далее проверять регулярно на наличие заболеваний, передаваемых половым путем, дать противозачаточные таблетки и т.д.), и предоставить ей **юридическую помощь.**

Необходимо поддерживать осторожное равновесие между предоставлением жертве нападения необходимой медицинской помощи со стороны соответствующих специалистов и принятием организацией необходимых мер поддержки.

См. также Предупреждение и реагирование на нападения в Главе 5.

[2] Большая часть этих сведений заимствована нами из книги Ван Брабанта (Van Brabant) «Operational Security in Violent Environments», из World Vision и из руководств по безопасности Всемирного совета церквей (World Council of Churches' Security Manuals).

ДЕКЛАРАЦИЯ О ЗАПРЕЩЕНИИ НАСИЛИЯ ПРОТИВ ЖЕНЩИН (1993) ОПРЕДЕЛЯЕТ НАСИЛИЕ ПРОТИВ ЖЕНЩИНЫ КАК:

Любой акт насилия, связанный с половой принадлежностью, который приводит или может привести к физическому, сексуальному или психологическому ущербу или страданию женщин, включая угрозы совершения таких актов, принуждение или насильственное лишение свободы, совершаемые публично или в частной жизни (Статья 1).

Насилие против женщины подразумевает, среди прочего, следующее:

а) • Физическое, сексуальное и психологическое насилие, совершаемое в семье, включая избиение, сексуальные извращения в отношении детей женского пола, насилие, связанное с приданым, супружеское изнасилование, нанесение увечий женским половым органам и другие традиционные практики, наносящие ущерб женщине; а также несупружеское насилие и насилие, связанное с эксплуатацией.

б)•Физическое, сексуальное и психологическое насилие, совершаемое в обществе, включая изнасилование, сексуальные извращения, сексуальные домогательства и запугивания на работе, в учебных заведениях и других местах, торговля женщинами и принудительная проституция.

в)• Физическое, сексуальное и психологическое насилие, совершаемое при попустительстве государства, независимо от того, где оно совершается. (Статья 2).

Глава 11

Безопасность в зонах вооруженных конфликтов

Цель

Снижение риска, являющегося неотъемлемой частью вооруженных конфликтов.

Риск в конфликтных ситуациях

Работа в зонах конфликтов подвергает правозащитников особому риску, особенно в ситуациях, связанных с вооруженными противостояниями, для которых характерно большое количество жертв среди гражданского населения, связанное с неразборчивостью в ведении военных действий и по другим причинам, в результате которых гражданские лица становятся объектами непосредственного нападения. Для придания этим фактам широкой гласности требуются политические меры.

И хотя вы не в состоянии контролировать военные действия, вы можете адаптировать свое поведение, чтобы не пострадать от этого конфликта, или принять адекватные меры в случае какого-либо происшествия.

Если вы постоянно находитесь в районе, в котором регулярно происходят вооруженные конфликты, вы, вероятно, установите много контактов, необходимых для продолжения вашей работы, для собственной защиты, для защиты вашей семьи и людей с которыми вы работаете.

Тем не менее, если вы работаете в зоне вооруженного конфликта, где вы находитесь не постоянно, то с самого начала вы должны **ответить для себя на три важных вопроса:**

а • Какой уровень риска вы готовы на себя взять? Это касается как отдельного человека, так и всей организации, в которой вы работаете.

б • Перевешивают ли преимущества вашего пребывания в этой зоне тот риск, которому вы себя подвергаете?
Перспективные цели работы по защите прав человека не могут достигаться ценой высокого риска.

в • Простое «знание зоны конфликта» или «хорошее знание оружия» не защитит вас, если по вам откроют огонь, или вы подвергнетесь миномётному обстрелу, или попадете под пулю снайпера.

Виды обстрела

Вы можете попасть под обстрел из автоматических винтовок, пулемётов, минометов, снарядов, бомб и ракет с суши, воздуха и моря. Обстрел может быть более или менее прицельным, начиная от снайперского и заканчивая обстрелом с вертолетов; он может производиться в условиях хорошей видимости, с корректировкой минометного огня или в виде заградительного артиллерийского огня. Это может быть также массированный артиллерийский огонь для сплошного поражения всей зоны.

Чем прицельнее обстрел, тем меньшему риску вы подвергаетесь, при условии, что огонь направлен не на вас, не на ту территорию, где вы находитесь и не на прилегающую к ней территорию. В этом случае риск может снизиться, если вы покинете этот участок. **В любом случае, помните, что если вы попали под обстрел, трудно определить направлен он на вас или нет. Выяснение этого факта не является приоритетным, как вы увидите ниже.**

Принятие мер предосторожности: Снижение вашей уязвимости для обстрела

1 • Избегайте опасных мест

Избегайте расквартирования, размещения офисов или пребывания в течение длительного времени вблизи возможных объектов нападения, таких как гарнизоны или средства телекоммуникации, в зонах боевых действий или действий террористов. То же самое относится к стратегическим районам, таким как подъезды к городу и выезды из него, аэропорты или места, обеспечивающие выгодные позиции для контроля над окружающей территорией.

2 • Найдите адекватную защиту от нападения

Осколки стекла, вылетающие из ближайших окон при обстреле, являются одной из основных причин ранений. Прикрытие окон картоном или наклеивание на них липкой ленты позволяет снизить эту опасность. В случае нападения, отойдите от окон и укройтесь на полу, под столом или в помещении с толстыми стенами, а еще лучше - в подвале.

Иногда очень полезны мешки с песком, но только в том случае, если и другие здания также обложены мешками с песком, в противном случае вы рискуете привлечь к себе ненужное внимание.

Если в вашем распоряжении ничего нет, то лягте на пол или в любое углубление на земле – это обеспечит хотя бы частичную защиту.

Простая кирпичная стена или дверца автомобиля не защитят вас от винтовочной пули или от огня из более тяжелого оружия. Артиллерийские снаряды или ракеты способны убить на расстоянии нескольких километров, поэтому вы можете пострадать, даже не находясь вблизи зоны обстрела.

Взрывы бомб или минометных снарядов могут причинить вред вашему слуху: прикройте уши обеими руками и приоткройте рот.

Наглядное обозначение вашего офиса, местонахождения или транспорта может быть полезным, **но только в тех случаях, когда нападающие относятся к вашей работе с уважением.** В противном случае вы подвергнете себя излишнему риску. Если вы хотите привлечь к себе внимание, сделайте это при помощи флага (флажка) или цветовых обозначений и знаков, нанесенных на стены или крышу (если есть опасность воздушного нападения).

3 ◆ Передвижение автотранспортом

Если вы находитесь в автотранспорте, который подвергся прямому обстрелу, вы можете попробовать оценить ситуацию, но точная оценка ситуации в этот момент весьма затруднена. Как правило, **будет логичным предположить, что автомобиль стал или станет мишенью, и поэтому будет правильным покинуть его и немедленно спрятаться в укрытие.** Автомобиль представляет собой заметную цель. Он уязвим и помимо риска, связанного с прямым обстрелом, подвергает вас опасности поражения стеклом или последствиями взрыва топливного бака. Если обстрел ведется с большой дистанции, попробуйте продолжать движение в автомобиле до ближайшего укрытия.

Мины и неразорвавшиеся артиллерийские снаряды[1]

Мины и неразорвавшиеся артиллерийские снаряды представляют серьезную угрозу гражданским лицам в зонах вооруженных конфликтов. Они могут быть следующими:

- **Мины:**
  - Противотанковые мины устанавливаются на дорогах и путях сообщения и способны уничтожить обычный автомобиль.
  - Противопехотные мины меньше и потенциально могут устанавливаться в любых местах, через которые проходят люди. Большинство противопехотных мин зарывается в землю. Не забывайте, что люди устанавливающие мины на дороге, могут также заминировать прилегающее к ней поле и ближайшие просёлки.
- **Мины-ловушки:**
  - Мины-ловушки – это небольшие взрывные устройства, спрятанные в предметах, выглядящих повседневными или даже привлекательными (например, с яркой окраской), которые взрываются при прикосновении к ним. Этот термин используется также для мин, соединенных с каким-либо предметом, который можно передвигать или привести в действие (т.е. всё, что угодно - от трупа до брошенной автомашины).
- **Неразорвавшиеся снаряды:**
  - Этот термин применяется для обозначения любого боеприпаса, который был выпущен, но не разорвался.

Превентивные меры против неразорвавшихся снарядов и мин

Единственный способ избежать заминированных участков – это знать их расположение. Если вы находитесь в этом районе не постоянно и не живете здесь, вы можете выяснить расположение минных полей только путем активных расспросов местных жителей или специалистов, если в этом районе уже имели место обстрелы и боевые действия. Лучше использовать асфальтированные шоссе, легко проходимые и регулярно используемые дороги, а также передвигаться по следу других автомобилей. **Никогда не покидайте автотрассы с машиной или без неё, не приближайтесь к бордюрному камню и не выходите на обочину.** Там могут находиться неразорвавшиеся снаряды или скрытые мины или другие взрывные устройства, которые остаются активными в течение многих лет.

[1] Многое из изложенной в данном разделе информации заимствовано из прекрасного руководства Конрада ван Брабанта (Koenraad van Brabant) «Operational Security Management in Conflict Areas [Оперативное управление безопасностью в конфликтных зонах]» (см. раздел Избранная библиография).

Неразорвавшиеся снаряды могут оказаться в любой местности, в которой прошли обстрелы или боевые действия и иногда их можно даже обнаружить визуально. Золотое правило: **не приближайтесь к ним, не прикасайтесь к ним, по возможности отметьте место их нахождения и немедленно сообщите об их обнаружении.**

Мины-ловушки обычно обнаруживаются в местах, покинутых вооруженными формированиями. В этих зонах важно ни к чему не прикасаться и не передвигать предметы, а также держаться подальше от покинутых зданий.

Подрыв автомобиля или человека на мине

Существует два золотых правила:

- Там, где есть одна мина – будут ещё мины.
- Никогда не действуйте импульсивно, даже если имеются раненые.

Если вам необходимо отступить, отходите по своим следам, если они видны. Если вы передвигаетесь с помощью автотранспорта и подозреваете присутствие противотанковых мин, выйдите из машины и вернитесь по следу автомобиля.

Если движение в сторону потерпевшего или отход из заминированной территории – единственный выход в сложившейся ситуации, встаньте на колени или лягте на землю и начинайте зондировать грунт небольшим заостренным предметом (очень тонким кусочком дерева или металла), осторожно втыкая его в землю под углом 30° и осторожно нащупывая присутствие любых твердых предметов. В случае обнаружения какого-либо твердого предмета, очень осторожно очистите его с одной стороны, пока не увидите, что это за предмет. Мины могут также приводиться в действие с помощью растяжек-ловушек. При обнаружении проволочных растяжек не отрезайте их.

Всё это, конечно, может занять значительное время[2].

[2] Руководство и информацию по вопросам связанным с минами вы можете найти на веб-странице Международной кампании по запрещению мин (International Campaign to Ban Landmines): www.icbl.org

Безопасная связь и информационные технологии

(подготовлено при содействии организации "Приватерра" – www.privaterra.org)

Цель

Существующий в мире большой разрыв в информационных технологиях оказывает негативное влияние и на правозащитников. Эта глава в основном посвящена информационным технологиям, то есть компьютерам и Интернету[1]. Правозащитники, не имеющие доступа к компьютерам или Интернету, могут не иметь доступа к необходимой им информации. В то же время, они испытывают острую потребность в новыхс редствах связи и в знаниях по использованию информационных технологий для защиты прав человека.

Руководство по проблемам безопасности средств связи и по их предупреждению

Знание – это сила, и зная свои потенциальные проблемы, связанные с безопасностью средств связи, вы можете чувствовать себя более защищёнными при выполнении работы. Ниже приводятся несколько способов получения незаконного доступа к вашей информации и средствам связи и противодействия им, а также некоторые меры по их предупреждению.

Разговоры

Для того, чтобы получить незаконный доступ к информации, необязательно, чтобы она проходила через Интернет. При обсуждении важной информации, задумайтесь над следующим:

1. Доверяете ли вы людям, с которыми ведете разговор?
2. Нужна ли им та информация, которую вы им предоставляете?
3. Находитесь ли вы в безопасном окружении? «Жучки» и другие подслушивающие устройства часто специально устанавливаются в местах, которые люди считают безопасными, таких как частные офисы, оживленные улицы, спальни и автомобили.

[1]Настоящая глава основана на работе Роберта Гуэрры, Катицы Родригес и Карин Младен (Robert Guerra, Katitza Rodríguez and Caryn Mladen) из организации "Приватерра" - НПО, работающей по всему миру в области безопасности и информационных технологий для правозащитников посредством организации курсов и предоставления консультаций. В настоящее время «Приватерра» работает над более подробным руководством по электронным средствам связи для Фонда «Фронт Лайн», которое будет опубликовано в 2005 г. (в этой главе в отдельных местах текст незначительно упрощён Энрике Эгуреном).

Возможно, будет трудно найти ответ на третий вопрос, поскольку микрофоны или «жучки» могут быть установлены в комнате с целью передачи или записи всего, что там говорится. Кроме того, для прослушивания разговоров с большого расстояния могут устанавливаться лазерные микрофоны, направленные на окна. Тяжелые портьеры, а также окна с двойными рамами обеспечивают некоторую защиту от лазерных «жучков». Некоторые безопасные здания имеют двойные окна, чтобы исключить риск прослушивания с помощью лазерных устройств.

Что можно сделать?

- **Всегда исходите из того, что кто-то прослушивает ваш разговор.** С таким подходом "здоровой паранойи" вы будете более осторожным при обсуждении конфиденциальных вопросов.

- **Специальные приборы для обнаружения «жучков» могут помочь,** но они могут быть дорогими и их может быть трудно достать. Кроме того, иногда люди, нанимаемые для обнаружения и устранения «жучков», имеют самое непосредственное отношение к их установке. При проведении проверки на их наличие, они находят несколько «одноразовых» "жучков" (дешевые "жучки", устанавливаемые специально, чтобы их обнаружили) или, как ни удивительно, ничего не находят и говорят, что ваш офис «чист».

- **Любой персонал по уборке помещений может представлять серьезную угрозу безопасности.** У этого персонала есть возможность для внеурочного доступа к вашему офису и для того, чтобы каждую ночь выносить все, что вы выбрасываете в корзины. Весь персонал должен проходить регулярную проверку на безопасность, так как уже после поступления на работу в вашу организацию члены обслуживающего персонала могут быть скомпрометированы.

- **Как можно чаще меняйте помещения, где проводятся совещания.** Чем больше помещений или комнат используется для проведения совещаний или обсуждений, тем больше потребуется людей и оборудования для ведения прослушивания.

- **Помните о подарках, которые предназначены для того, чтобы они всегда были при вас**, таких как дорогие ручки, булавки или броши, или другие вещи, либо о подарках, предназначенных для офиса, таких как красивые пресс-папье или большие картины. В прошлом эти предметы широко использовались для прослушивания разговоров.

- **Исходите из того, что определенная часть вашей информации подвергается прослушиванию** в любое время. Возможно, вы захотите чаще менять свои планы и коды, чтобы прослушивающие могли получить только обрывки подлинной информации. Рассмотрите возможность передачи фальшивой информации, чтобы проверить воспользуется ли ею кто-то и отреагирует ли на неё.

- Дли максимального снижения эффективности лазерных микрофонов, **обсуждайте конфиденциальные вопросы в подвале или в помещении без окон.** Некоторые лазерные подслушивающие устройства могут быть менее эффективны в грозу и при других атмосферных изменениях.

- **Включите аудиозапись «белого шума» или популярную песню для** создания помех. Только дорогостоящие технологии способны отделять посторонние шумы от разговора.

- **Широкие открытые пространства могут быть как союзниками, так и врагами.** Проведение встречи в укромном месте дает возможность обнаружить слежку и наблюдение за вами, но затрудняет возможность затеряться в толпе. Легче всего затеряться в толпе, но в этом случае также намного легче вас увидеть и подслушать.

Мобильные телефоны

Все телефоны могут прослушиваться, если прослушивающие лица имеют достаточные технические возможности. Нельзя исходить из того, что телефонный разговор не прослушивается. В этом плане, аналоговые мобильные телефоны менее безопасны, чем цифровые, и оба типа менее безопасны по сравнению с наземными линиями связи.

С помощью сотового наблюдения, можно определить как ваше местонахождение, так и содержание вашего разговора. Для определения вашего местонахождения вам не обязательно говорить по телефону – это можно сделать в любое время, если ваш телефон включен.

Не храните такую конфиденциальную информацию как имена, номера телефонов и т.д. в памяти вашего телефона. В случае кражи вашего телефона, эта информация может быть использована для установления местонахождения людей, которым вы хотите помочь, и нанесения им ущерба.

Физическая безопасность информации в офисе

Всегда держите офис закрытым, включая двери и окна. Пользуйтесь ключами, которые требуют специального разрешения на изготовление их дубликатов и ведите учет всех дубликатов ключей. НЕ ДАВАЙТЕ ключи третьим лицам, даже обслуживающему персоналу и ремонтникам. Обязательно присутствуйте лично или обеспечьте присутствие кого-либо из коллег, которым вы доверяете, когда в помещении находятся третьи лица. Если это невозможно, убедитесь, что у вас есть комната с ограниченным доступом для хранения конфиденциальных документов. Проверяйте, надёжно ли закрыты все двери офиса, и убедитесь, что в оставленных после рабочего дня бумажных отходах нет конфиденциальных документов.

Используйте канцелярскую бумагорезательную машину с поперечной порезкой для уничтожения листов бумаги, содержащих конфиденциальную информацию. Канцелярская бумагорезательная машина с продольной порезкой в большинстве случаев бесполезна. Для уничтожения особо секретной информации обеспечьте сожжение порезанных листов бумаги, измельчение золы и смыв её в унитаз.

Основные правила безопасности при работе с компьютером и файловыми документами[2]

Уходя из офиса, по возможности, всегда запирайте компьютер. Поверните экран компьютера в сторону от окна.

На все розетки установите стабилизаторы напряжения (колебания напряжения способны повредить ваш компьютер).

Храните резервные носители информации, включая информацию на бумаге, в отдельном надежном месте. Убедитесь, что ваши резервные носители информации находятся в безопасности на компьютере, и доступ к его жесткому диску зашифрован и поддерживается надежной организацией резервного копирования, либо что компьютеры защищены сложными физическими замками.

Для снижения риска несанкционированного доступа к вашему компьютеру установите на него пароль и всегда выключайте его, когда уходите.

Зашифруйте свои файлы, на случай если кто-нибудь получит доступ к вашему компьютеру и обойдет установленный пароль.

[2] Более подробную информацию по безопасности компьютера можно найти в Фонде «Фронт Лайн», обратившись по адресу: info@frontlinedefenders.org или в организации «Приватерра», обратившись по адресу: info@privaterra.org

Если ваш компьютер украли или сломали, вы сможете восстановить свои файлы, если ежедневно создаете надежные резервные копии. Храните свои зашифрованные копии за пределами офиса и в надежном месте.

Стертые файлы невозможно восстановить, если вы стерли их с помощью программы PGP Wipe или другой подобной программы, а не сбросили их просто в «Корзину» вашего компьютера.

Ваш компьютер может быть запрограммирован на отправку ваших файлов или на получение с него информации иным способом - без вашего ведома. Чтобы избежать этого, следует приобретать компьютер только в надежном месте; после приобретения сразу переформатируйте его жесткий диск и только после этого устанавливайте необходимое вам программное обеспечение. К обслуживанию компьютера допускайте только проверенных специалистов, и, тем не менее, все время присматривайте за ними.

Предусмотрите возможность отключения телефона/модема от вашего компьютера или иного способа отключения от Интернета, когда вы вынуждены оставлять компьютер без присмотра. Это позволит нейтрализовать жульнические программы, настроенные на работу в ночное время. Никогда не оставляйте компьютер включенным, когда вы покидаете офис на весь день. Изучите возможность установки специального программного обеспечения, способного исключить доступ к компьютеру через определенное время. Это позволит защитить ваш компьютер в то время, когда вы пьете кофе или снимаете фотокопию документа.

В ваших веб-предпочтениях активируйте функцию показа расширения файлов, чтобы определить тип файла до его открытия. Вам не нужна вирусная программа, запускаемая открытием исполняемого файла, который вы считали простым текстовым файлом. В Internet Explorer войдите в меню Tools (Сервис) и выберите позицию Folder Options (Меню Папка). Кликните View (Вид) и убедитесь, что в окне Hide extensions for known file types (Скрыть расширения для известных типов файлов) установлено NOT (НЕТ).

Проблемы безопасности, связанные с использованием Интернета

Ваша почта не отправляется непосредственно с вашего компьютера на компьютер вашего адресата. Она проходит через несколько взаимосвязанных узлов связи, оставляя при прохождении информацию о себе. **Доступ к этой информации можно получить на всем пути её прохождения (а не только на её выходе / входе из страны/в страну)!**

Кто-то может заглядывать через ваше плечо, когда вы набираете текст. Это особенно актуально в Интернет-кафе. Если у вас имеется связь с Интернет, ваша почта может быть доступной любому человеку в вашем офисе. Ваш системный администратор может иметь особые преимущества доступа ко всей почте.

Ваш провайдер услуг Интернета (ISP) имеет доступ к вашей почте, и любой, кто имеет на него влияние, может оказать на него давление, чтобы вынудить провайдера направлять ему копии всей вашей электронной корреспонденции или заблокировать прохождение части ваших отправлений.

При прохождении через Интернет ваша почта проходит через сотни небезопасных сторонних субъектов. Хакеры могут получить доступ к вашим коммуникациям по мере их прохождения. Провайдер Интернет-связи вашего получателя, сеть и офис получателя вашей почты также могут иметь свои уязвимые места.

Основные правила безопасности в Интернет

Вирусы и другие жульнические программы, такие как «троянские кони», или «троянцы», могут появиться отовсюду; даже ваши друзья могут неосознанно переслать вам вирусы со своих компьютеров. Пользуйтесь надежными антивирусными

программами и постоянно обновляйте их в автоматическом режиме. Новые вирусы создаются и обнаруживаются постоянно, поэтому регулярно посещайте Библиотеку информации о вирусах (Virus Information Library) на веб-сайте www.vil.nai.com и загружайте свежие программы для защиты от новых вирусов.

Обычно вирусы передаются через электронную почту, поэтому придерживайтесь правил безопасной связи (см. ниже). Вирусы – это разовые программы, предназначенные для самостоятельного тиражирования, они могут быть вредными и безвредными. «Троянцы» – это программы, предназначенные для того, чтобы третья сторона (или кто-либо ещё) имела доступ к вашему компьютеру.

Хорошие брандмауэры (аппаратно-программные средства межсетевой защиты) могут помочь вам стать невидимыми для хакеров и предупредить вторжение посторонних лиц в вашу систему. Это гарантирует, что только специально допущенный персонал может выйти в Интернет с вашего компьютера и не позволит таким программам, как «троянцы», отправлять информацию или открывать «черный ход» в ваш компьютер, через который могут войти хакеры.

Система "регистрации клавиатуры" следит за любыми вашими действиями на клавиатуре. Эти программы вводятся кем-то, когда вас нет, или с помощью вируса или «троянца», которые попадают в вашу систему через Интернет. Система "Регистрации клавиатуры" следит за любыми вашими действиями на клавиатуре и сообщает о вашей работе, обычно, через Интернет. С этими программами можно бороться с помощью установки паролей защиты, соблюдения практики безопасной отправки сообщений, применения антивирусных программ и использования программ с управлением от мыши для ввода пароля. Нейтрализовать системы "регистрации клавиатуры" можно также с помощью вашего физического отключения от Интернета, обычно, простым отключением телефонной связи от вашего компьютера, когда вы на нём не работаете.

Почтовый адрес может быть "ложным" (поддельным), т.е. помимо истинного владельца им может воспользоваться кто-то ещё. Это может быть сделано путем взлома сетей провайдера и получения доступа к чужому компьютеру и паролю, или путем использования адреса, который может быть похож на адрес какого-либо конкретного человека. Например, путем замены нижнего регистра буквы "l" на цифру "1" вы можете создать похожий адрес, и большинство людей не заметят разницы. Чтобы избежать розыгрыша, используйте набор слов, составляющих смысл, и периодически задавайте вопросы, на которые может ответить только настоящий владелец адреса. Просите подтверждения любых подозрительных запросов информации путем проверки через другие формы связи.

Не позволяйте никому заглядывать на свою страничку быстрого просмотра ваших обращений к WWW-серверу и стирайте вашу кэш-память после каждого подключения к Интернету. В Internet Explorer выберите меню Tools (Сервис), затем Options (Настройки). В Netscape Navigator перейдите к Edit (Правка), затем к Preferences (Параметры). Когда вы находитесь в любом из этих меню, сотрите всю вашу ретроспективу работы, все выходы в Интернет и очистите вашу кэш-память. Помните, что необходимо также стереть все ваши закладки. На вашей страничке быстрого просмотра хранятся также записи о сайте, который вы посещаете в кэш-файлах, поэтому определите, какие файлы должны быть уничтожены в вашей системе.

Обновите все веб-системы быстрого просмотра для поддержки 128-битовой кодировки. Это поможет обезопасить любую информацию, которую вы хотите передать по веб-сети, включая пароль и другую конфиденциальную информацию, представленную в виде специальных форм. Установите самые последние пачи безопасности (программы, исправляющие ошибки, найденные изготовителем в своей программной продукции – Прим. пер.) для всего используемого программного обеспечения, особенно для таких пакетов, как Microsoft Office, Microsoft Internet Explorer и Netscape.

Не пользуйтесь компьютером с хранящейся в нем конфиденциальной информацией для быстрого просмотра несущественных веб-сайтов.

Основные правила безопасной работы с электронной почтой

Ниже приведены основные правила безопасной работы с почтой, которые должны соблюдаться вами, вашими друзьями и коллегами. Сообщите им, что вы не станете читать их сообщения, если они не станут придерживаться безопасной практики пользования электронной почтой.

1• НИКОГДА не вскрывайте почту от людей, которых вы не знаете.

2• НИКОГДА не пересылайте почту от людей, которых вы не знаете, или если её автором является кто-то, кого вы не знаете. Все эти письма, рассылаемые с пометками "думайте о хорошем", могут содержать вирусы. Направляя их вашим друзьям и коллегам, вы можете занести вирусы в их компьютеры. Если вам нравится их сентиментальность, наберите заново сообщение и направьте его сами. Если набор сообщения не заслуживает вашего времени, то, вероятно, это не столь важное сообщение.

3• НИКОГДА не загружайте и не открывайте приложений, если не знаете их содержания и не уверены в том, что оно безопасно. Отключите опцию автоматической загрузки в вашей компьютерной программе. Многие вирусы и «троянцы» распространяются сами по себе в виде "червей", и современные «черви» часто рассылаются теми, кого вы знаете. Умные «черви» сканируют вашу адресную книгу, особенно если вы пользуетесь программами Microsoft Outlook или Outlook Express и маскируются под обычные приложения, полученные от обычных отправителей. PGP-подписывание почты с приложениями и без них способно снять проблемы, связанные с освобождением от вирусов приложений, отправляемых вами своим коллегам (PGP – программа кодирования информации, см. ниже в разделе "Кодирование").

4• НЕ пользуйтесь форматами HTML, MIME или RTF при отправке вашей почты - пользуйтесь только простым текстом. Расширенные письма могут содержать встроенные программы, которые могут обеспечить доступ к вашей информации или повредить ваши компьютерные файлы.

5• При пользовании программами Outlook или Outlook Express, отключите опции предварительного просмотра на экране.

6• Шифруйте вашу почту всякий раз, когда это возможно. Незашифрованная почта подобна открытке, которую может прочитать каждый, кто её увидит или получит к ней доступ. Зашифрованная почта – это письмо, надежно спрятанное в конверте.

7• Используйте в заглавии темы что-нибудь значимое, чтобы читатель знал, о чем будет говориться в сообщении. Скажите вашим друзьям и коллегам, чтобы в заглавии темы они всегда писали о чем-нибудь личном, чтобы вы знали, что сообщение действительно пришло от них. В противном случае, кто-то может прислать сообщение от их имени либо «троянец», возможно, разослал инфицированную программу по всем адресам их адресной книги, включая вас. Тем не менее, не пользуйтесь заглавиями, которые выдают конфиденциальную информацию, зашифрованную в почтовом сообщении. Помните, что указываемая вами тема сообщения не шифруется и может привести к разглашению характера зашифрованного письма, что, в свою очередь, может привести к проведению акта агрессии. Многие хакерские программы в настоящее время автоматически сканируют и копируют почтовые сообщения с "интересными" темами, такими как "отчет", "конфиденциально", "личное" и с другими признаками, указывающими на то, что сообщение представляет для кого-то определенный интерес.

8• НИКОГДА не направляйте почту большой группе адресатов, указанных в строках "To" или "CC". Лучше направьте сообщение самому себе и включите всех остальных в строки "bcc". Это признак хороших манер, а также хороший способ сохранения конфиденциальности.

В противном случае, вы направляете МОЙ почтовый адрес людям, которых Я не знаю; это порочная и оскорбительная практика, которая потенциально чревата опасностями и представляет угрозу.

9 • НИКОГДА не отвечайте на спам (веерная рассылка рекламной информации), даже с просьбой удалить вас из списка рассылки. Серверы спама рассылают сообщения по огромному количеству адресов, и они никогда не знают, какой из них является «активным» (имеется ввиду некто, кто активно использует ваш электронный адрес). Получая ваше сообщение, сервер воспринимает вас как «активного» пользователя и, в результате, вы можете получить ещё больше спама, чем раньше.

10 • Если это возможно, заведите себе отдельный компьютер, не подключенный к остальным компьютерам, который принимает обычные почтовые сообщения и не содержит файлов с данными.

Кодирование: Вопросы и ответы

Ниже приводится список наиболее часто задаваемых вопросов с ответами на них. По всем вопросам просим также обращаться в НПО "Приватерра"через веб-сайт www.privaterra.org

В: Что такое кодирование?

О: Кодирование означает преобразование данных в секретный код, который никто не может расшифровать, кроме лица, для которого эта информация предназначается. При наличии достаточного количества времени и вычислительных способностей можно прочесть все закодированные сообщения, но это может потребовать много времени и ресурсов. Проще говоря, кодирование - это способ, с помощью которого вы можете защитить ваши файлы и почту от посторонних глаз. Ваши файлы переводятся в код, представляющий собой, на первый взгляд, произвольное сочетание букв и цифр, которые непонятны для тех, кто их видит. Для того, чтобы закодировать файл, вы «закрываете» его ключом, в виде пароля. Для того, чтобы закодировать сообщение, вы закрываете его с помощью пары ключей, используя свой пароль. Сообщение может быть открыто только тем лицом, для которого оно предназначено, с помощью его / её пароля.

В: Почему правозащитники должны пользоваться кодированием?

О: Кодированием должны пользоваться все, так как цифровые средства связи изначально не обеспечивают конфиденциальности. Кроме того, правозащитники подвержены большему риску, чем большинство людей, и их файлы и средства связи более уязвимы. Для правозащитников чрезвычайно важно пользоваться кодированием для собственной защиты и для защиты людей, которым они стремятся помочь.

Цифровая технология - одно из благ, которым пользуются правозащитники. Она обеспечивает быструю связь, более высокую эффективность работы и расширяет их возможности. Однако, при всех своих достоинствах, эта технология представляет также определенную опасность. Тот факт, что вы одели ремень безопасности еще не означает, что вы ожидаете аварии всякий раз, когда вы находитесь за рулем. Управление автомобилем в более опасной ситуации, такой как автогонки, ещё больше побуждает вас пристегнуть ремень для ещё большей безопасности.

Правозащитники часто становятся объектами слежки. И поскольку практически каждый имеет возможность получить доступ к незакодированным сообщениям и прочитать их, то почти неизбежно, что ваши незакодированные сообщения будут прочитаны на каком-то этапе пересылки. Не исключено, что ваши сообщения уже контролируются вашими оппонентами, и вы никогда об этом не узнаете. Оппоненты людей, которым вы хотите помочь – это также и ваши оппоненты.

В: Является ли использование кодирования нелегальным?

О: Иногда. Применение кодирования вполне легально в большинстве стран мира. Тем не менее, есть исключения. В Китае, например, организации должны получить специальное разрешение на использование кодирования, и при въезде в эту страну вы должны декларировать технологию кодирования, используемую на вашем портативном компьютере. Сингапур и Малайзия имеют законы, требующие, чтобы каждый, кто хочет использовать кодирование, сообщил о своих личных паролях. Аналогичные законы действуют в Индии. Есть также и другие исключения.

Информационный центр электронной конфиденциальности (EPIC) предлагает «International Survey of Encryption Policy [Обзор международный политики в области кодирования]», в котором ведется обсуждение законов, действующих в большинстве стран мира на сайте http://www2.epic.org/reports/crypto2000/. Последний раз этот перечень обновлялся в 2000 г. Если вас интересуют более современные данные в этой сфере, проконсультируйтесь в "Приватерре, прежде чем использовать кодирование в какой-либо конкретной стране.

В: Что необходимо сделать, чтобы обезопасить наши IT-системы?

О: Это зависит от вашей системы и от вашей деятельности, но, как правило, каждый должен иметь следующее:

- Брандмауэр.
- Дисковое кодирование.
- Почтовое кодирование, позволяющую выполнять цифровую подпись, такую как PGP.
- Программы обнаружения вирусов.
- Надежную систему резервного копирования: Отправляйте все материалы на безопасный сайт и каждую неделю создавайте резервную копию на CD-RW и храните её в отдельном безопасном месте.
- Пароли, которые можно запомнить, но трудно угадать.
- Иерархию доступа– не у всех сотрудников организации есть необходимость в доступе ко всем файлам.
- Последовательность – инструментальные средства не будут работать, если вы не работаете с ними постоянно!

Но наличие нужного программного обеспечения ещё не обеспечивает решения всех проблем. Как правило, **самым слабым звеном являются не технологии, а люди.** Кодирование не даст результатов, если люди не пользуются им постоянно, если они сообщают случайным знакомым свои пароли или оставляют их на видных местах, например, на наклейках на мониторе. Наличие резервной копии не спасет вас в случае пожара или нападения, если вы не храните её в отдельном безопасном месте. Доступ к конфиденциальной информации должен основываться на принципе необходимости, а не должен быть открыт всем без исключения сотрудникам организации, поэтому вам необходимо создать иерархии и правила. В целом, важно очень сознательно и скрупулёзно относиться к вопросам конфиденциальности и безопасности в своей повседневной работе. Мы называем это "здоровой паранойей".

В: Как определить какую программу кодирования выбрать?

О: Обычно, вы можете спросить об этом у своих друзей, и получить подтверждение у нас. Вам необходимо связываться с определенными людьми и группами, поэтому если они используют специальные системы кодирования, то для удобства связи вам

следует пользоваться такими же системами. Однако, прежде свяжитесь с нами. Некоторые пакеты программного обеспечения не очень эффективны, а некоторые представляют собой «сыр в мышеловке». Эти пакеты привлекают вас тем, что они бесплатны и, на первый взгляд, представляют собой безупречное программное обеспечение, предлагаемое теми самыми людьми, которые хотят шпионить за вами. Можно ли придумать лучший способ получения доступа к вашим наиболее уязвимым средствам связи, чем контролировать ваше программное обеспечение по кодированию?! Тем не менее, существует много популярных торговых марок - как лицензионного программного обеспечения, так и бесплатных программных средств. Но помните - перед тем, как использовать их, следует разузнать о них как можно больше[3].

В: Не приведет ли использование кодирования к ещё большему риску взлома моего компьютера?

О: Никто не узнает, что вы пользуетесь кодированием, если за вашей перепиской ранее не была установлена слежка. Если слежка установлена, то вашу частную переписку уже давно читают. Это значит, что взлом уже совершен людьми, ведущими за вами слежку. Здесь есть опасность того, что люди, ведущие за вами наблюдение, в случае потери возможности читать вашу почту, попробуют прибегнуть к другим вариантам, поэтому вам следует хорошо знать своих коллег и пользоваться безопасным способом создания резервных копий и кодирования своей информации.

(Примечание: У нас нет информации о случаях, когда использование шифровальных программ приводило к возникновению проблем у правозащитников. Тем не менее, прежде чем приступить к шифровке информации, тщательно проанализируйте такую возможность, особенно если вы находитесь в стране с серьезным вооруженным конфликтом – военная разведка может заподозрить вас в передаче военной информации или, если шифровку используют очень немногие правозащитники, это привлечет к вам ненужное внимание.)

В: Почему необходимо все время кодировать почту и документы?

О: Если вы используете кодирование только в сугубо конфиденциальных целях, то те, кто ведет слежку за вами или вашими клиентами, смогут догадаться, когда происходят важные события, и вероятность нанесения удара в это время возрастет. Они не смогут прочесть вашу закодированную переписку, но смогут определить, закодирована она или нет. Внезапное широкое применение кодирования может привести к нападению, поэтому лучше начать использование кодирования до начала специального проекта. Практически, лучше всего, если передача информации осуществляется равномерно. Отсылайте закодированную почту с регулярным интервалом, даже если вам нечего сообщить. В этом случае, если вам будет необходимо отправить конфиденциальную информацию, она пройдет более незаметно.

В: Если у меня есть брандмауэр, зачем мне кодировать свою почту?

О: Брандмауэр предотвращает доступ хакеров к вашему жесткому диску и сети, но когда вы отправляете сообщение в Интернет, оно становится доступным всем. Поэтому перед отправкой вам следует его защитить.

В: Никто не взламывает мой офис, почему же я должен пользоваться конфиденциальным программным обеспечением?

О: Вы не знаете, взламывает ли кто-нибудь вашу систему либо считывает информацию с вашего компьютера. Без шифрования переписки, физической безопасности или правил конфиденциальности любой может получить доступ к вашим файлам, читать вашу почту и использовать ваши документы в корыстных интересах без вашего ведома. Ваши незакодированные письма могут также поставить под угрозу других людей, особенно в тех местах, где политически мотивированные нападения имеют большую вероятность. Вы должны шифровать свои файлы так же, как вы запираете свою входную дверь.

[3] Например, программа PGP ("Pretty Good Privacy" [Весьма хорошая конфиденциальность]) - хорошо известная и безопасная система. Вы можете загрузить её с веб-сайта www.pgpi.org

В: У нас нет доступа к Интернету, и мы вынуждены пользоваться услугами Интернет-кафе. Как нам защитить нашу почту, отправляемую с чужого компьютера?

О: Вы, тем не менее, можете шифровать вашу почту и файлы. Прежде чем идти в Интернет-кафе, зашифруйте все файлы, которые вы хотите отправить и скопируйте их в таком виде на дискету или компакт-диск. В Интернет-кафе подпишитесь на услугу шифрования, такую как www.hushmail.com или на любую услугу, обеспечивающую анонимность отправителя, такую как www.anonymizer.com, и пользуйтесь ими при отправке своей почты. Убедитесь, что люди, получающие вашу почту, также пользуются этими услугами.

В: Если так важно защитить наши файлы и почту, почему все не делают этого?

О: Эта сравнительно новая технология, но её применение расширяется. Банки, многонациональные корпорации, информационные агентства и правительства пользуются кодированием, считая это правильным вкладом капитала и неизбежными издержками при ведении бизнеса. НПО подвержены большему риску, чем компании, которые пользуются поддержкой большинства правительств. НПО значительно чаще становятся объектами наблюдения и, поэтому, должны быть более активны в применении этой технологии. Правозащитники заинтересованы в защите преследуемых людей и групп. С этой целью они создают файлы, позволяющие идентифицировать и установить местонахождение людей. В случае несанкционированного доступа к этим файлам, этих людей могут убить, замучить, похитить или «уговорить» больше не сотрудничать с НПО. Информация с этих файлов может быть также использована как свидетельские показания против НПО и их клиентов для осуществления политических преследований.

В: Один из наших принципов – открытость. Мы выступаем за большую прозрачность деятельности правительства. Как мы можем пользоваться секретными технологиями?

О: Защита информации совместима с открытостью. Если правительство пожелает открыто запросить вашу информацию, оно может сделать это в соответствии с установленными процедурами. Технологии защиты препятствуют несанкционированному доступу к вашей информации.

В: Мы соблюдаем все протоколы конфиденциальности и секретности, но, тем не менее, происходит утечка информации – в чём дело?

О: Возможно, в вашей организации есть шпион, или кто-то просто не может хранить конфиденциальную информацию. Пересмотрите вашу информационную иерархию, сократите список людей, имеющих доступ к конфиденциальной информации – и возьмите этих немногих людей под особое наблюдение. Большие корпорации и организации обычно передают небольшие объемы фальшивой информации конкретным людям. Если происходит утечка этой информации, то её можно легко проследить к работнику, которому эта ложная информация предоставлялась.

Рекомендации по использованию шифрования

- Пользуйтесь шифрованием постоянно. Если вы шифруете только конфиденциальные материалы, то тот, кто отслеживает вашу почту, будет знать, когда должно произойти что-то важное. Внезапное увеличение количества зашифрованной информации может привести к нападению на офис.

- НЕ сообщайте о конфиденциальной информации в теме сообщения, которая, как правило, не кодируется, даже если само сообщение закодировано.

- Применяйте пароли, содержащие буквы, числа, пунктуацию и пробелы, о которых можете знать только вы. Некоторые способы безопасного создания пароля используют компоновки на клавиатуре или произвольный набор слов вперемежку с символами. Практически, чем длиннее пароль, тем он надежнее.

- НЕ используйте в качестве пароля одно слово, имена, известные фразы или адреса, записанные в вашей адресной книге. Такие пароли расшифровываются в течение нескольких минут.

- Создайте резервную копию ключа кодирования (файла, в котором находится ваш личный ключ для кодирования программ) в безопасном месте, например, на гибком диске или на маленькой удаляемой «цепочке» в памяти флэш-карты.

- НЕ отправляйте конфиденциальный материал людям только потому, что они прислали вам зашифрованное сообщение с указанием знакомого вам имени. Любой человек может "разыграть" вас, сделав свой адрес похожим на адрес человека, которого вы знаете. Всегда проверяйте идентичность этого человека, прежде чем доверять ему – свяжитесь с ним лично, проверьте по телефону или направьте ещё одно сообщение для двойной проверки.

- Учите других пользоваться шифрованием. Чем больше людей им пользуется, тем в большей безопасности будут все.

- НЕ забывайте подписывать и шифровать сообщение. Ваш получатель должен знать, не подменили ли сообщение при пересылке.

- Обязательно шифруйте файлы, направляемые в виде отдельных приложений. Обычно, они шифруются автоматически при отправке зашифрованного письма.

Руководство по безопасному управлению офисом и информацией

Безопасное управление офисом

Безопасное управление офисом связано с соблюдением установленного порядка. Установленный порядок управления может иметь не только плюсы, но и минусы. Для разработки позитивных методов управления офисом полезно ознакомиться с тем, что за ними стоит. Мы составили список привычек, которые могут быть вам полезны для более безопасного управления информацией, но только в том случае, если вы их разовьете и задумаетесь над тем, почему они важны.

Что является наиболее важным для секретности и безопасности в управлении офиса?

- Всегда помнить об информации и о том, кто имеет к ней доступ
- Развивать безопасные привычки и постоянно их соблюдать
- Правильно пользоваться инструментальными средствами

Администрирование

Многие организации имеют системных администраторов или сотрудника, имеющего административный доступ к почтовым сообщениям, сетевым компьютерам и контролирующего установку новых программ. Если кто-то уходит из организации или отсутствует, то администратор может получить доступ к информации этого человека, и работа продолжается непрерывно. Это также означает, что этот сотрудник несет ответственность за чистоту программного обеспечения и за то, что оно получено из надежных источников.

Проблема заключается в том, что некоторые организации рассматривают эту функцию как простую техническую поддержку и разрешают посторонним контракторам пользоваться административными привилегиями. Этот администратор имеет фактический контроль над всей информацией в организации и должен пользоваться абсолютным доверием. Некоторые организации делят эту функцию между двум лицами: руководителем организации и другим доверенным лицом.

Некоторые организации предпочитают кодировать и хранить все PGP-ключи и пароли в удаленном и безопасном месте в другой организации, которой они доверяют. Это позволяет избежать проблем, если кто-то забыл свой пароль или потерял свой персональный ключ. Тем не менее, местонахождение файлов должно гарантировать их абсолютную конфиденциальность и безопасность; необходимо также вести специальные протоколы по получению доступа к файлам.

Правила:

1 • НИКОГДА не предоставляйте административных привилегий посторонним контракторам. Не только потому, что им следует доверять меньше, чем людям, работающим в организации, но ещё и потому, что в случае необходимости, с ними труднее связаться.

2 • Административные привилегии должны предоставляться только самым доверенным лицам.

3 • Определите объем информации, к которому системный администратор может иметь доступ: доступ ко всем компьютерам, к паролям, к паролям логина, к ключам и паролям PGP и т.д.

4 • Если вы решите хранить копии паролей и персональных ключей PGP в другой организации, то вы должны составить правила допуска к ним.

5 • В случае увольнения человека из организации, его пароли и коды допуска должны быть немедленно изменены.

6 • Если кто-то, имеющий административные привилегии, увольняется из организации, все пароли и коды доступа должны быть немедленно изменены.

Управление программным обеспечением

Использование «пиратских» программ может создать для организации угрозу со стороны так называемой «программной полиции». Официальные власти могут применить санкции против организации за пользование нелегальными программами, наложить огромные штрафы и даже закрыть их. Организация, попавшая под подозрение, не пользуется сочувствием и поддержкой у западных средств информации, так как это расценивается не как атака на саму правозащитную организацию, а как атака на «пиратство». Будьте очень осторожны в вопросах лицензий на пользование программами и не разрешайте всем сотрудникам офиса подряд делать их копии. Кроме того, «пиратские» программы могут быть небезопасны, так как могут содержать вирусы. При инсталляции новых программ всегда используйте антивирусные утилиты.

Системный администратор должен контролировать инсталляции новых программ, чтобы вначале убедиться, что они проверены. Не допускайте инсталляции потенциально небезопасных программ и устанавливайте только те программы, которые действительно необходимы.

Устанавливайте самые последние пачи безопасности (программы, исправляющие ошибки, найденные изготовителем в собственной программной продукции) для всех используемых программ, особенно для Microsoft Office, Microsoft Internet Explorer и Netscape. Самую большую угрозу для безопасности представляют программы и аппаратное управление, поставляемые с известными недостатками. Лучше всего, продумайте целесообразность подключения к программному обеспечению с открытым ключом, которое не зависит от модели коммерческого поведения "Безопасность за счёт неясности", а скорее приглашает как экспертов по безопасности, так и хакеров к тщательной проверке всех кодов. Использование программного обеспечения с открытым ключом и любого другого программного обеспечения, кроме продукции фирмы Microsoft, дает дополнительные преимущества защиты от стандартных вирусов и хакеров-любителей. Количество вирусов, созданных для операционных систем Linux или Macintosh меньше, так как большинство людей пользуются оболочкой Windows. Outlook – наиболее распространенная почтовая программа, и, поэтому, она чаще всего подвергается атакам со стороны хакеров.

Полезные привычки при работе с электронной почтой

Шифрование почты должно стать привычкой. Легче помнить, что шифровать надо всё, чем соблюдать правила, когда шифровать почту, а когда нет. Помните, если почта шифруется всегда, то лица, просматривающие вашу почту, никогда не смогут определить, когда она становится более важной и конфиденциальной, а когда нет.

Несколько важных советов:

- Всегда сохраняйте зашифрованную почту в зашифрованном виде. Вы всегда сможете её расшифровать позже, в противном случае, если кто-то получит доступ к вашему компьютеру, то она станет такой же уязвимой, как и любая незашифрованная информация.

- Будьте последовательны со всеми, с кем вы обмениваетесь зашифрованной информацией, чтобы быть уверенными, что они не расшифровывают и не пересылают почту другим лицам или отвечают, не шифруя свою почту. Лень – самая большая опасность в обмене информацией.

- Возможно, вы захотите создать несколько безопасных учётных записей для электронной почты, обычно не используемых и неохваченных серверами спама, для тех сотрудников, которые находятся непосредственно на месте событий. Эти почтовые адреса должны постоянно проверяться, но не использоваться никем, кроме соответствующих сотрудников. Таким образом вы сможете уничтожить электронные адреса, на которые приходит большое количества спама, не подвергая при этом никакому риску свою контактную базу.

Общие соображения относительно использования Интернет-кафе и др.

Почта, отправленная простым или незашифрованным текстом, может быть доступна различным посторонним лицам, если они того захотят. Один из них может быть вашим провайдером Интернет-услуг (ISP) или любым другим ISP, через который проходит ваша почта. Почта проходит через множество серверов по пути от отправителя к получателю, она игнорирует геополитические границы и может проходить через серверы в других странах, даже если вы отправляете их в пределах одной страны.

Несколько общих советов по вопросам, которые обычно неправильно понимаются пользователями Интернета.

- Пароль, защищающий файл, настолько малоэффективен, что вряд ли

его стоит ставить для защиты документа содержащего конфиденциальную информацию. Он дает только ложное ощущение безопасности.

- Архивирование файла не защитит его от того, кто захочет узнать, что там внутри.

- Если вы хотите быть уверенным, что файл или письмо отправлено безопасно, используйте шифрование (см www.privaterra.com).

- Если вы хотите безопасно отправить письмо или документ, используйте шифрование очень последовательно, вплоть до конечного получателя. Не следует направлять закодированное письмо с места событий в Нью-Йорк, Лондон или в другие пункты назначения, а потом пересылать это же письмо в незашифрованном виде по другому адресу.

- Интернет – это глобальная по своей природе сеть. И нет разницы между пересылкой письма из одного офиса в Манхэттене в другой и пересылкой письма из Интернет-кафе в Южной Африке на компьютер в Лондоне.

- Используйте шифрование как можно чаще, даже если почта или пересылаемые данные не являются конфиденциальными!

- Убедитесь, что ваш компьютер оснащён антивирусной программой. Многие вирусы создаются с целью получения информации из вашего компьютера, включая содержание жестких дисков, почты и адресной книги.

- Убедитесь, что ваше программное обеспечение защищено лицензией. Если вы пользуетесь нелицензионными программами, то, в глазах правительства и средств массовой информации, вы сразу становитесь «пиратом», а не правозащитником. Лучше всего пользоваться программным обеспечением с открытым ключом – оно бесплатно!

- Не существует 100%-й безопасности, если вы пользуетесь Интернетом. Помните, что кто-то может получить доступ к вашей системе, используя метод «социального хакера», выдавая себя за кого-то другого по телефону или по электронной почте. Пользуйтесь своим собственным суждением и здравым смыслом.

Генеральная Ассамблея A/RES/53/144

Пятьдесят третья сессия

РЕЗОЛЮЦИЯ, ПРИНЯТАЯ ГЕНЕРАЛЬНОЙ АССАМБЛЕЕЙ

53/144. Декларация о праве и обязанности отдельных лиц, групп и органов общества поощрять и защищать общепризнанные права человека и основные свободы

Генеральная Ассамблея,

подтверждая важное значение соблюдения целей и принципов Устава Организации Объединенных Наций для поощрения и защиты всех прав человека и основных свобод всех лиц во всех странах мира,

ссылаясь на резолюцию 1998/7 Комиссии по правам человека от 3 апреля 1998 года1, в которой Комиссия одобрила текст проекта декларации о праве и обязанности отдельных лиц, групп и органов общества поощрять и защищать общепризнанные права человека и основные свободы,

ссылаясь также на резолюцию 1998/33 Экономического и Социального Совета от 30 июля 1998 года, в которой Совет рекомендовал Генеральной Ассамблее для принятия проект декларации,

сознавая важность принятия проекта декларации в контексте пятидесятой годовщины Всеобщей декларации прав человека2,

1. утверждает Декларацию о праве и обязанности отдельных лиц, групп и органов общества поощрять и защищать общепризнанные права человека и основные свободы, прилагаемую к настоящей резолюции;

2. предлагает правительствам, учреждениям и организациям системы Организации Объединенных Наций и межправительственным и неправительственным организациям активизировать их усилия по распространению Декларации и содействию ее всеобщему уважению и пониманию и просит Генерального секретаря включить текст Декларации в следующее издание сборника «Права человека: сборник международных договоров».

85-е пленарное заседание,
9 декабря 1998 года.

Приложение
Декларация о праве и обязанности отдельных лиц, групп и органов общества поощрять и защищать общепризнанные права человека и основные свободы

Генеральная Ассамблея,

подтверждая важное значение соблюдения целей и принципов Устава Организации Объединенных Наций для поощрения и защиты всех прав человека и основных свобод всех лиц во всех странах мира,

подтверждая также важное значение Всеобщей декларации прав человека и Международных пактов о правах человека как основных элементов международных усилий по содействию всеобщему уважению и соблюдению прав человека и основных свобод и важное значение других договоров о правах человека, принятых в рамках системы Организации Объединенных Наций, а также на региональном уровне,

подчеркивая, что все члены международного сообщества должны, совместно и по отдельности, выполнять свое торжественное обязательство по поощрению и содействию уважению прав человека и основных свобод для всех без какого бы то ни было различия, в том числе по признаку расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения, и подтверждая особое значение обеспечения международного сотрудничества для выполнения этого обязательства в соответствии с Уставом Организации Объединенных Наций,

1См. Официальные отчеты Экономического и Социального Совета, 1998 года, Дополнение N°3 (E/1998/23), глава II, раздел A.
2 Резолюция 217 A (III)
3 Резолюция 2200 A (XXI), приложение.

признавая важную роль международного сотрудничества и ценную работу отдельных лиц, групп и ассоциаций по содействию эффективному устранению всех нарушений прав человека и основных свобод народов и отдельных лиц, в том числе массовых, грубых или систематических нарушений, таких, как нарушения, которые являются результатом апартеида, всех форм расовой дискриминации, колониализма, иностранного господства или оккупации, агрессии или угроз национальному суверенитету, национальному единству или территориальной целостности, а также результатом отказа признать право народов на самоопределение и право каждого народа на осуществление полного суверенитета над своими богатствами и природными ресурсами,

признавая взаимосвязь между международным миром и безопасностью и осуществлением прав человека и основных свобод и сознавая, что отсутствие международного мира и безопасности не является оправданием их несоблюдения,

вновь заявляя, что все права человека и основные свободы являются универсальными, неделимыми и взаимозависимыми и взаимосвязанными и должны поощряться и осуществляться на справедливой и равноправной основе без ущерба для осуществления каждого из этих прав и свобод,

подчеркивая, что основная ответственность и обязанность поощрять и защищать права человека и основные свободы лежит на государстве,

признавая право и обязанность отдельных лиц, групп и ассоциаций поощрять уважение и содействовать более глубокому осмыслению прав человека и основных свобод на национальном и международном уровнях,

заявляет:

Статья 1

Каждый человек имеет право, индивидуально и совместно с другими, поощрять и стремиться защищать и осуществлять права человека и основные свободы на национальном и международном уровнях.

Статья 2

1. Каждое государство несет основную ответственность и обязанность защищать, поощрять и осуществлять все права человека и основные свободы, в частности путем принятия таких мер, какие могут потребоваться для создания всех необходимых условий в социальной, экономической и политической, а также в других областях и правовых гарантий, необходимых для обеспечения того, чтобы все лица под его юрисдикцией, индивидуально и совместно с другими, могли пользоваться всеми этими правами и свободами на практике.

2. Каждое государство принимает такие законодательные, административные и иные меры, какие могут оказаться необходимыми для обеспечения эффективных гарантий прав и свобод, упомянутых в настоящей Декларации.

Статья 3

Внутреннее законодательство, согласующееся с Уставом Организации Объединенных Наций и другими международными обязательствами государства в области прав человека и основных свобод, образует юридические рамки, в которых должны осуществляться и обеспечиваться права человека и основные свободы и в которых

должна проводиться вся упомянутая в настоящей Декларации деятельность по поощрению, защите и эффективному осуществлению этих прав и свобод.

Статья 4

Ничто в настоящей Декларации не может толковаться как наносящее ущерб или противоречащее целям и принципам Устава Организации Объединенных Наций либо как ограничивающее или умаляющее положения Всеобщей декларации прав человека$_2$, Международных пактов о правах человека3 и других международных договоров и обязательств, применимых в этой области.

Статья 5

В целях поощрения и защиты прав человека и основных свобод каждый человек имеет право, индивидуально и совместно с другими, на национальном и международном уровнях:

a) проводить мирные встречи или собрания;

b) создавать неправительственные организации, ассоциации или группы, вступать в них и участвовать в их деятельности;

c) поддерживать связь с неправительственными или межправительственными организациями.

Статья 6

Каждый человек, индивидуально и совместно с другими, имеет право:

a) знать, искать, добывать, получать и иметь в своем распоряжении информацию о всех правах человека и основных свободах, включая доступ к информации о том, каким образом обеспечиваются эти права и свободы во внутреннем законодательстве, в судебной или административной системах;

b) как предусматривается в международных договорах о правах человека и других применимых международных договорах, свободно публиковать, передавать или распространять среди других мнения, информацию и знания о всех правах человека и основных свободах;

c) изучать, обсуждать, составлять и иметь мнения относительно соблюдения всех прав человека и основных свобод как в законодательстве, так и на практике, и привлекать внимание общественности к этим вопросам, используя эти и другие соответствующие средства.

Статья 7

Каждый человек имеет право, индивидуально и совместно с другими, развивать и обсуждать новые идеи и принципы, касающиеся прав человека, и добиваться их признания.

Статья 8

1. Каждый человек имеет право, индивидуально и совместно с другими, иметь реальный доступ на недискриминационной основе к участию в управлении своей страной и ведении государственных дел.

2. Это включает, в частности, право, индивидуально и совместно с другими, представлять в правительственные органы и учреждения, а также в организации, занимающиеся ведением государственных дел, критические замечания и предложения

относительно улучшения их деятельности и привлекать внимание к любому аспекту их работы, который может затруднять или сдерживать поощрение, защиту и осуществление прав человека и основных свобод.

Статья 9

1. При осуществлении прав человека и основных свобод, включая поощрение и защиту прав человека, упомянутых в настоящей Декларации, каждый человек, индивидуально и совместно с другими, имеет право на пользование эффективными средствами правовой защиты и на защиту в случае нарушения этих прав.

2. С этой целью каждый человек, чьи права или свободы предположительно нарушены, имеет право лично или через посредство законно уполномоченного представителя направить жалобу в независимый, беспристрастный и компетентный судебный или иной орган, созданный на основании закона, рассчитывать на ее безотлагательное рассмотрение этим органом в ходе публичного разбирательства и получить от такого органа, в соответствии с законом, решение, предусматривающее меры по исправлению положения, включая любую надлежащую компенсацию, в случае нарушения прав или свобод этого лица, а также право на принудительное исполнение этого решения или постановления без неоправданной задержки.

3. С этой же целью каждый человек, индивидуально и совместно с другими, имеет, в частности, право:

a) в связи с нарушениями прав человека и основных свобод в результате политики и действий отдельных должностных лиц и государственных органов подавать жалобы или иные соответствующие обращения в компетентные национальные судебные, административные или законодательные органы или в любой другой компетентный орган, предусмотренный правовой системой государства, которые должны вынести свое решение по данной жалобе без неоправданной задержки;

b) присутствовать на открытых слушаниях, разбирательствах и судебных процессах с целью сформировать свое мнение об их соответствии национальному законодательству и применимым международным обязательствам и принципам;

c) предлагать и предоставлять профессиональную квалифицированную правовую помощь или иные соответствующие консультации и помощь в деле защиты прав человека и основных свобод.

4. С этой же целью и в соответствии с применимыми международными договорами и процедурами, каждый человек имеет право, индивидуально и совместно с другими, на беспрепятственный доступ к международным органам, обладающим общей или специальной компетенцией получать и рассматривать сообщения по вопросам прав человека и основных свобод, а также поддерживать с ними связь.

5. Государство проводит незамедлительное и беспристрастное расследование или обеспечивает проведение расследования всякий раз, когда имеются разумные основания полагать, что на любой территории, находящейся под его юрисдикцией, произошло нарушение прав человека и основных свобод.

Статья 10

Никто не должен участвовать, посредством действия или несовершения требуемого действия, в нарушении прав человека и основных свобод и никто не может подвергаться какому-либо наказанию или преследованию за отказ от участия в этом.

Статья 11

Каждый человек, индивидуально и совместно с другими, имеет право на законном основании заниматься своим родом деятельности или работать по профессии. Каждый, кто по роду своей профессии может влиять на человеческое достоинство,

права человека и основные свободы других лиц, должен уважать эти права и свободы и соблюдать соответствующие национальные и международные стандарты поведения или этики, которые связаны с родом занятий или профессией.

Статья 12

1. Каждый человек имеет право, индивидуально и совместно с другими, участвовать в мирной деятельности, направленной против нарушений прав человека и основных свобод.

2. Государство принимает все необходимые меры в целях обеспечения защиты, с помощью компетентных органов, любого человека, выступающего индивидуально и совместно с другими, от любого насилия, угроз, возмездия, негативной дискриминации де-факто или де-юре, давления или любого иного произвольного действия в связи с законным осуществлением его или ее прав, упомянутых в настоящей Декларации.

3. В этой связи каждый человек, индивидуально и совместно с другими, имеет право на эффективную защиту национального законодательства в случае принятия ответных мер или выступлений с использованием мирных средств против деятельности или действий, вменяемых государству, результатом которых являются нарушения прав человека и основных свобод, а также против актов насилия, совершаемых группами или отдельными лицами и затрагивающих осуществление прав человека и основных свобод.

Статья 13

Каждый имеет право, индивидуально и совместно с другими, запрашивать, получать и использовать ресурсы специально для целей поощрения и защиты прав человека и основных свобод мирными средствами в соответствии со статьей 3 настоящей Декларации.

Статья 14

1. Государство несет ответственность за принятие законодательных, судебных, административных или иных надлежащих мер в целях содействия пониманию всеми лицами, находящимися под его юрисдикцией, своих гражданских, политических, экономических, социальных и культурных прав.

2. Такие меры включают, в частности:

a) публикацию и широкое распространение национальных законов и положений, а также основных международных договоров о правах человека;

b) полный и равный доступ к международным документам в области прав человека, включая периодические доклады государства органам, учрежденным на основании международных договоров о правах человека, участником которых оно является, а также краткие отчеты об обсуждениях и официальные доклады этих органов.

3. Государство обеспечивает и поддерживает, когда это необходимо, создание и развитие новых независимых национальных учреждений по вопросам поощрения и защиты прав человека и основных свобод на всей территории, находящейся под его юрисдикцией, таких, как омбудсмены, комиссии по правам человека или любые другие формы национальных учреждений.

Статья 15

Государство несет ответственность за поощрение и содействие преподаванию прав человека и основных свобод на всех уровнях образования и за обеспечение

включения всеми лицами, ответственными за подготовку юристов, сотрудников правоохранительных органов, военнослужащих и государственных служащих, в свои учебные программы соответствующих элементов преподавания прав человека.

Статья 16

Отдельные лица, неправительственные организации и соответствующие учреждения играют важную роль в содействии более глубокому пониманию общественностью вопросов, связанных со всеми правами человека и основными свободами, посредством такой деятельности, как образование, профессиональная подготовка и исследования в этих областях в целях обеспечения, в частности, более глубокого понимания и укрепления терпимости, мира и дружественных отношений между государствами и между всеми расовыми и религиозными группами, с учетом различных особенностей, характерных для обществ и коллективов, в которых они осуществляют свою деятельность.

Статья 17

При осуществлении прав и свобод, упомянутых в настоящей Декларации, каждый человек, действующий индивидуально или совместно с другими, подвергается только таким ограничениям, которые согласуются с соответствующими международными обязательствами и которые установлены законом исключительно в целях обеспечения должного признания и уважения прав и свобод других лиц и удовлетворения справедливых требований нравственности, общественного порядка и общего благосостояния в демократическом обществе.

Статья 18

1. Каждый человек имеет обязанности перед обществом и в обществе, в котором только и возможно свободное и полное развитие его личности.

2. Отдельным лицам, группам, учреждениям и неправительственным организациям надлежит играть важную роль и нести ответственность в деле обеспечения демократии, поощрения прав человека и основных свобод и содействия поощрению и развитию демократических обществ, институтов и процессов.

3. Аналогичным образом, им надлежит играть важную роль и нести ответственность в деле содействия, в соответствующих случаях, поощрению прав каждого человека на социальный и международный порядок, при котором могут быть полностью реализованы права и свободы, закрепленные во Всеобщей декларации прав человека и других договорах в области прав человека.

Статья 19

Ничто в настоящей Декларации не может толковаться как означающее, что какое-либо лицо, группа или орган общества или какое-либо государство имеет право заниматься какой-либо деятельностью или совершать какие-либо действия, направленные на ликвидацию прав и свобод, упомянутых в настоящей Декларации.

Статья 20

Ничто в настоящей Декларации не может также толковаться как разрешающее государствам поддерживать и поощрять деятельность отдельных лиц, групп лиц, учреждений или неправительственных организаций, противоречащую положениям Устава Организации Объединенных Наций.

ИЗБРАННАЯ БИБЛИОГРАФИЯ И ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

ИЗБРАННАЯ БИБЛИОГРАФИЯ

- Amnesty International (2003): "Essential actors of our time. Human rights defenders in the Americas". AI International Secretariat (Index AI: AMR 01/009/2003/s).

- AVRE and ENS (2002): "Afrontar la amenaza por persecución sindical". Escuela de Liderazgo Sindical Democrático. Published by the Escuela Nacional Sindical and Corporación AVRE. Medellín, Colombia.

- Bettocchi, G., Cabrera, A.G., Crisp, J., and Varga, A (2002): "Protection and solutions in situations of internal displacement". EPAU/2002/10, UNHCR.

- Cohen, R. (1996): "Protecting the Internally Displaced". World Refugee Survey.

- Conway, T., Moser, C., Norton, A. and Farrington, J. (2002) "Rights and livelihoods approaches: Exploring policy dimensions". DFID Natural Resource Perspectives, no. 78. ODI, London.

- Dworken, J.T "Threat assessment". Series of modules for OFDA/InterAction PVO Security Task Force (Mimeo, included in REDR Security Training Modules, 2001).

- Eguren, E. (2000): "Who should go where? Examples from Peace Brigades International", in "Peacebuilding: a Field Perspective. A Handbook for Field Diplomats", by Luc Reychler and Thania Paffenholz (editors). Lynne Rienner Publishers (London).

- Eguren, E. (2000), "The Protection Gap: Policies and Strategies" in the ODI HPN Report, London: Overseas Development Institute.

- Eguren, E. (2000), "Beyond security planning: Towards a model of security management. Coping with the security challenges of the humanitarian work". Journal of Humanitarian Assistance. Bradford, UK.
www.jha.ac/articles/a060.pdf

- Eriksson, A. (1999) "Protecting internally displaced persons in Kosovo".
http://web.mit.edu/cis/www/migration/kosovo.html#f4

- ICRC (1983): Fundamental Norms of Geneva Conventions and Additional Protocols. Geneva.

- International Council on Human Rights Policy (2002): "Ends and means: Human Rights Approaches to Armed Groups". Versoix (Switzerland). www.international-council.org

- Jacobsen, K. (1999) "A 'Safety-First' Approach to Physical Protection in Refugee

Camps". Working Paper # 4 (mimeo).

• Jamal, A. (2000): "Acces to safety? Negotiating protection in a Central Asia emergency. Evaluation and Policy Analysis Unit, UNHCR. Geneva.

• Lebow, Richard Ned and Gross Stein, Janice. (1990) "When Does Deterrence Succeed And How Do We Know?" (Occasional Paper 8). Ottawa: Canadian Inst. for Peace and International Security.

• Mahony, L. and Eguren, E. (1997): "Unarmed bodyguards. International accompaniment for the protection of human rights". Kumarian Press. West Hartford, CT (USA).

• Martin Beristain, C. and Riera, F. (1993): "Afirmacion y resistencia. La comunidad como apoyo". Virus Editorial. Barcelona.

• Paul, Diane (1999): "Protection in practice: Field level strategies for protecting civilians from deliberate harm". ODI Network Paper no. 30.

• SEDEM (2000): Manual de Seguridad. Seguridad en Democracia. Guatemala.

• Slim, H. and Eguren, E. (2003): "Humanitarian Protection: An ALNAP guidance booklet". ALNAP. www.alnap.org.uk. London.

• Sustainable Livelihoods Guidance Sheets (2000). DFID. London, February 2000

• Sutton, R. (1999) The policy process: An overview. Working Paper 118. ODI. London.

• UNHCHR (2004): "About Human Rights Defenders" (extensive information): http://www.unhchr.ch/defenders/about1.htm

• UNHCHR (2004): "Human Rights Defenders: Protecting the Right to Defend Human Rights". Fact Sheet no. 29. Geneva.

• UNHCHR (2004): On women defenders: www.unhchr.ch/defenders/tiwomen.htm

• UNHCR (1999): Protecting Refugees: A Field Guide for NGO. Geneva.

• UNHCR (2001): Complementary forms of protection. Global Consultations on International Protection. EC/GC/01/18 4 September 2001

• UNHCR (2002) Strengthening protection capacities in host countries. Global Consultations on International Protection. EC/GC/01/19 * / 19 April 2002

• UNHCR-Department of Field Protection (2002) Designing protection strategies and measuring progress: Checklist for UNHCR staff. Mimeo. Geneva.

• Van Brabant, Koenraad (2000): "Operational Security Managment in Violent Environments". Good Practice Review 8. Humanitarian Practice Network. Overseas Development Institute, London.

• Vincent, M. and Sorensen, B. (eds) (2001) "Caught between borders. Response strategies of the internally displaced". Pluto Press. London.

Европейский отдел «Пис Бригейдс Интернешнл» с 2001г. предоставляет обучение и консультации по защите и безопасности правозащитников, в зависимости от располагаемого времени и средств.

Просим обращаться по электронной почте pbibeo@biz.tiscali.be, или пишите нам по адресу:
PBI- European Office, 38,
Rue Saint-Christophe, 1000 Bruxelles (Belgium)
Телефон/факс + 32 (0)2 511 14 98
www.peacebrigades.org/beo.html

Фонд «Фронт Лайн» предоставляет обучение в вопросах повышения безопасности и защиты правозащитников и издает тематические руководства и прочие материалы.

Дополнительные сведения указаны на сайте www.frontlinedefenders.org или их можно получить, обратившись по электронной почте info@frontlinedefenders.org или написав непосредственно по адресу:
Front Line, 16 Idrone lane, Off Bath Place, Blackrock, County Dublin, Ireland
тел: +353 1212 3750
fax: +353 1212 1001

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ