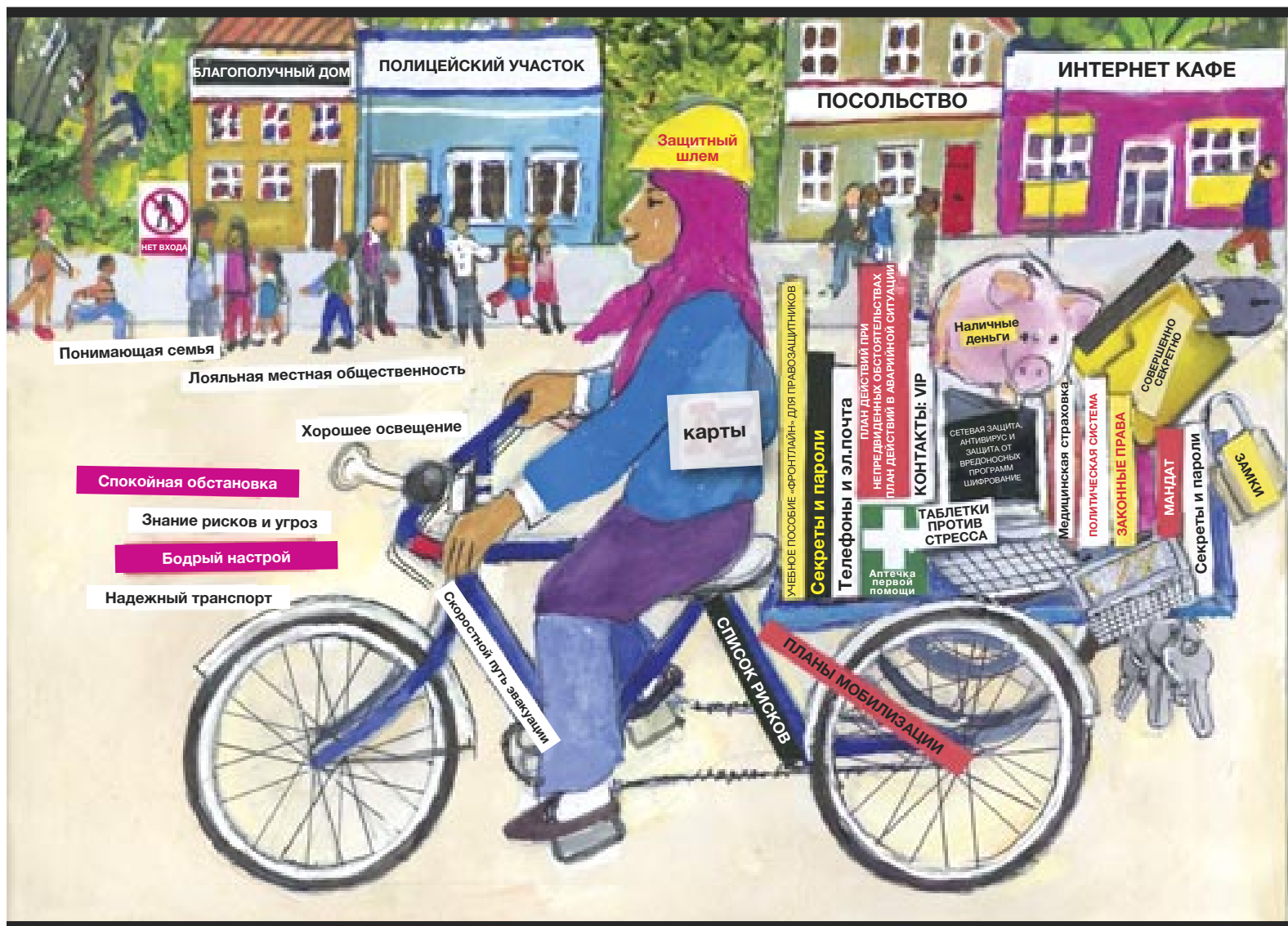


ПРАКТИЧЕСКОЕ УЧЕБНОЕ ПОСОБИЕ:

ПРАКТИЧЕСКИЕ МЕРЫ ДЛЯ ПРАВОЗАЩИТНИКОВ В ОПАСНОСТИ



ПРИЛОЖЕНИЕ 5

Контрольный список: Безопасность на работе

Этот контрольный список не предназначен для использования в качестве шаблона по безопасности. Обстоятельства в вашей конкретной ситуации являются ключевым определяющим фактором. Принимайте во внимание опасности и угрозы, с которыми вы сталкиваетесь, и любые имеющиеся уязвимые места, чтобы дополнить и персонализировать этот список.

1. Контактные лица в чрезвычайных ситуациях:

- Имеется ли удобный для применения и постоянно обновляемый список с телефонными номерами и адресами местных НПО, больниц с реанимационными отделениями, полиции, пожарной службы и службы скорой медицинской помощи?

2. Технические и физические границы (за пределами здания, внутри здания и внутри отдельных помещений):

- Проверьте состояние и исправность наружных ворот/ограды, дверей в здании, окон, стен и крыши;
- Проверьте состояние и исправность наружного освещения, аварийной сигнализации, камер или входных видеофонов;
- Проверьте наличие процедур пользования ключами, убедитесь, что ключи хранятся в надежном месте и имеют кодовую маркировку, что назначен ответственный за учет ключей, изготовление их дубликатов и исправность ключей и дубликатов. Проконтролируйте замену замков в случае потери или хищения ключа, а также создание записи об этом инциденте.
- Имеется ли специальная «безопасная» комната?
- Можно ли снять табличку с именем организации на время усиления угрозы, чтобы снизить уязвимость и возможность нападения?

3. Сотрудники офиса:

- Вы нанимаете только надежных людей, включая охранников, и проверяете их рекомендации?
- Все ли ваши сотрудники прошли обучение соответствующим планам безопасности?
- У вас есть план на случай налета на офис властями или другими группами?
- Используете ли вы «принцип служебной необходимости» (стратегия защиты информации, соответственно которой пользователь получает доступ только к данным, безусловно необходимым ему для выполнения конкретной функции) при выполнении особо секретной работы?
- Поддерживаете ли вы хорошие отношения с вашими сотрудниками, особенно, если вы знаете, что они испытывают финансовые или иные трудности? (Недовольные сотрудники могут стать очень опасными врагами).
- Когда кто-то уходит из организации, меняете ли вы меры безопасности, пароли, ключи согласно инструкциям?

4. Процедура приема посетителей и «фильтры»:

- Процедура приема применяется для всех типов посетителей? Весь ли персонал ознакомлен с ней?
- Интересуетесь ли вы у сотрудников, ведущих прием посетителей, работает ли процедура, и какие нужны улучшения?
- Знают ли сотрудники что делать при появлении неожиданного пакета/посылки? (например, изолировать его, не открывать, позвонить руководству).
- Записываете ли вы имена посетителей (включая тех, кто приходит на совещания в ваш офис)? Если да, то является ли эта информация секретной, и как вы ее защищаете? (например, кодированием или шифрованием файлов).

5. Безопасность информации (также см. Приложение 14 «Безопасность компьютерной и телефонной связи»)

- Выполняете ли вы регулярное копирование данных и сохраняете ли резервные копии в безопасном месте вне офиса?
- Знают ли сотрудники, что нельзя оставлять секретную информацию на своих столах?
- Имеется ли у вас система безопасности для записи конфиденциальной информации, например, о клиентах или свидетелях?
- Присваиваете ли вы своим (физическим или электронным) файлам с особо секретной информацией безопасные имена, чтобы их нельзя было сразу обнаружить?

6. Безопасность в чрезвычайной ситуации:

- Проверьте состояние огнетушителей, газовых вентилях/труб и водопроводных кранов, электрических предохранителей и кабелей, а также электрогенераторов (если применимо).

7. Ответственность и обучение:

- Были ли назначены ответственные за безопасность на работе? Было ли это эффективным?
- Имеется ли программа обучения безопасности на работе? Входят ли в нее все области, включая этот анализ? Все ли сотрудники прошли обучение? Было ли обучение эффективным?