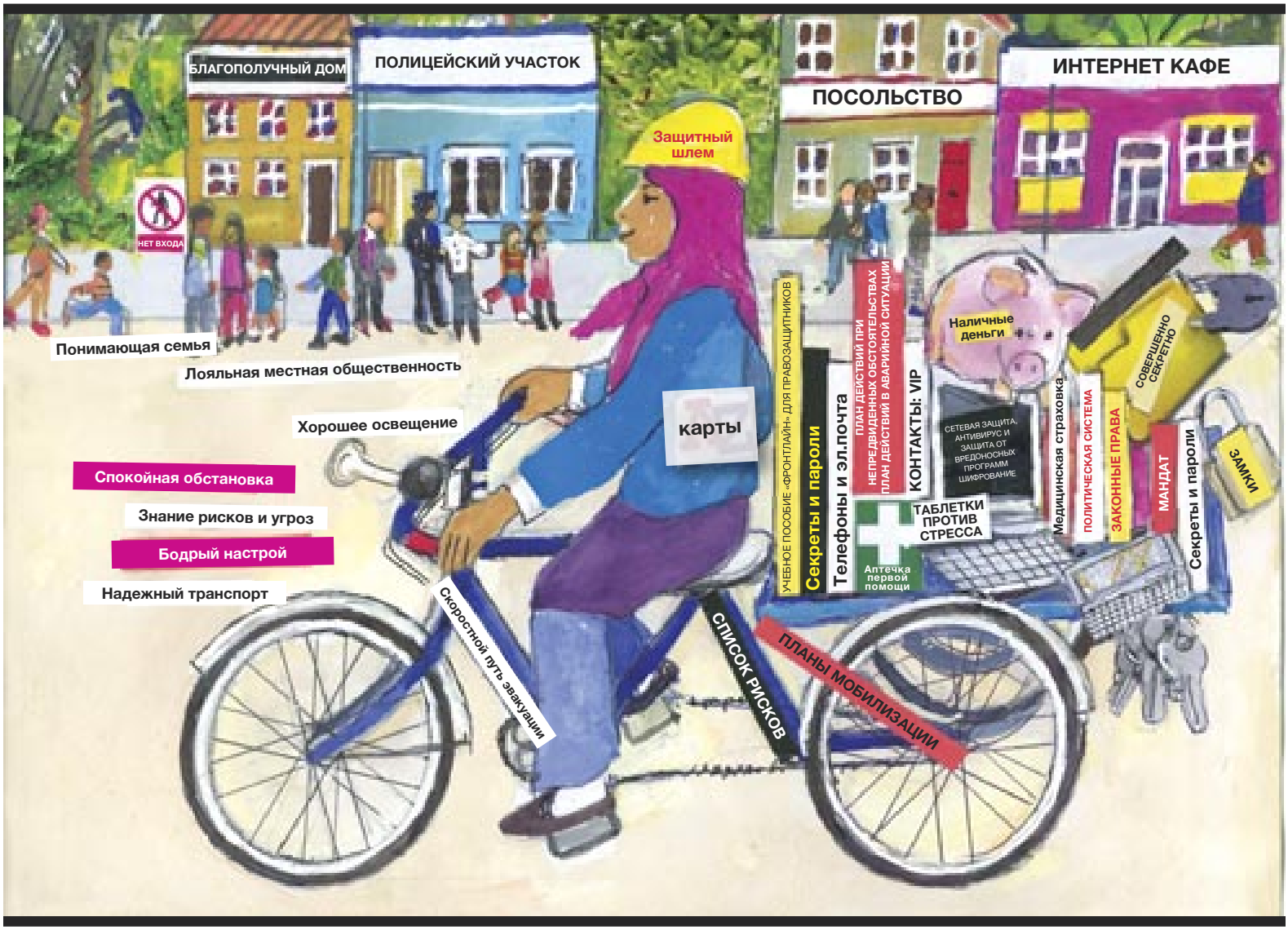
ПРАКТИЧЕСКОЕ УЧЕБНОЕ ПОСОБИЕ:

ПРАКТИЧЕСКИЕ МЕРЫ ДЛЯ ПРАВОЗАЩИТНИКОВ В ОПАСНОСТИ



FRONT LINE DEFENDERS

ПРИЛОЖЕНИЕ 14

Безопасность компьютерной и телефонной связи

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. Этот перечень является лишь списком ключевых пунктов.

Для получения детальной информации см. «Безопасность-в-коробке» по адресу: https://security.ngoinabox.org/

Эта информация включает советы, которые могут быть найдены в разделе «Карты осведомленности» проекта «Безопасность-в-коробке» – см. ссылку выше.

1. Защитите ваш компьютер от вредоносных программ и хакеров
- Установите антивирусные программы, антишпионские программы и брандмауэр.
- Не пользуйтесь пиратскими программами – это делает вас более уязвимым из-за отсутствия возможности их обновлений и потенциального обвинения в незаконном использовании программного обеспечения.
- Рассмотрите возможность использования бесплатного программного обеспечения с открытым кодом, такого как антивирусную программу AVAST, антишпионскую программу Spybot и брандмауэр Comodor.
- Рассмотрите возможность использования более безопасного браузера, такого как Firefox, который имеет встроенные системы безопасности (для получения дополнительной информации по защите своего компьютера см. https://security.ngoinabox.org/en/chapter-1)

2. Придумайте и регулярно обновляйте защитные пароли
- Чем длиннее будут ваши пароли, тем лучше. Ваши пароли должны быть длиннее 12 символов, содержать буквы верхнего и нижнего регистров, цифры и специальные знаки, а также символ пробела, если возможно.
- Желательно, чтобы ваши пароли не содержали словарных слов и/или публично известной информации о вас, такой как ваш день рождения или имя друга. Смешивайте слова или заменяйте слова специальными символами или номерами, можно использовать слова из разных языков.
- Обдумайте возможность использования какой-то фразы для создания вашего пароля. Это может быть заголовок книги или строка из песни (при этом буквы следует заменить цифрами или символами).
- Часто меняйте пароли.
- Составьте несколько надежных паролей для различных сервисов, регулярно обновляйте их, никому не сообщайте свои пароли (возможно, следует использовать программу KeePass для хранения своих паролей. Для дополнительной информации о программе KeePass см. https://security.ngoinabox.org/en/chapter-3)
- НИКОГДА никому не сообщайте свои пароли.
- НИКОГДА не разрешайте сайту или программе хранить ваши пароли

(для дополнительной информации о безопасности паролей см. https://security.ngoinabox.org/en/chapter-3)

3. Как защитить особо секретные файлы на вашем компьютере
- Регулярно создавайте резервные копии ваших файлов и храните их в безопасном месте.
- Давайте секретным файлам безопасные имена.
- Обдумайте возможность шифрования ваших файлов (имейте в виду, что шифрование является незаконным в некоторых странах и может привлечь к вам внимание).
- Бесплатное программное обеспечение с открытым кодом TrueCrypt может одновременно шифровать и скрывать ваши файлы.
- Удаленные файлы можно восстановить с вашего компьютера, поэтому обдумайте возможность использования безопасных инструментов удаления файлов, таких как CCleaner (для удаления временных файлов) и Eraser.
- Если возможно, проверьте репутацию вашего провайдера услуг сети Интернет или места, откуда вы выходите в Интернет, например, интернет-кафе.
- Убедитесь, что люди, с которыми вы общаетесь, также заботятся о своей безопасности и конфиденциальности. Общение – это двусторонний процесс. Безопасность теряет смысл, если только одна сторона заботится о сохранении конфиденциальности и безопасности

(для дополнительной информации см. (see https://security.ngoinabox.org/en/chapter-9 for more information).

4. Сохраняйте конфиденциальность ваших интернет-сессий
- Многие сервисы электронной почты небезопасны (включая Yahoo и Hotmail) и отображают ваш IP-адрес в сообщениях, которые вы отправляете. Сервисы электронной почты Gmail и Riseup более безопасны

(имейте в виду, что Google в прошлом уже уступал требованиям правительства, которые ограничивали свободу в цифровом пространстве).
- Использование услуг интернет-кафе может поставить вас под угрозу наблюдения. Осознавайте риски и понимайте, с кем и какой информацией вы делитесь. Удалите ваш пароль и историю посещений сайтов по завершении сеанса.
- При соединении с онлайн-сервисами, при возможности, используйте «https» вместо «http», тогда ваш логин, пароль и другая информация будет передаваться в защищенном виде.
- Не открывайте приложения, которые прикреплены к электронным письмам, полученных от незнакомых людей, или которые выглядят подозрительно.
- Будьте особенно осторожны, когда отправляете и получаете особо секретную информацию через Интернет.
- Старайтесь использовать прокси-сервер или приложения, которые делают анонимным ваш сеанс связи. Это позволит вам получать доступ к Интернету и осуществлять связь с использованием IP-адреса другого компьютера.
- Сервисы обмена мгновенными сообщениями (чаты) также недостаточно безопасны, хотя при этом Skype, вероятнее всего, безопаснее всех остальных
  (для дополнительной информации см. https://security.ngoinabox.org/en/chapter-7 и https://security.ngoinabox.org/en/chapter-8).

5. Социальные сети
- Хорошо обдумайте информацию, которую вы сообщаете о себе, вашем местонахождении, друзьях и т. д.
- Будьте аккуратны, если размещаете важную информацию, документы, фотографии и информацию о местонахождении других людей.
- Убедитесь, что ваши пароли надежны, и регулярно их меняйте.
- Будьте аккуратны, когда выходите на сайт вашей социальной сети через средства общего доступа к сети Интернет. Используйте их только в том случае, если им точно можно доверять. Удаляйте пароли и историю посещения сайтов после использования общего браузера или компьютера.
- Читайте и понимайте содержание таких документов как «Соглашения конечного пользователя», «Условия использования» и/или «Руководства по соблюдению конфиденциальности». Эти документы могут измениться в будущем, поэтому важно регулярно перечитывать новые версии.
- Убедитесь, что вы хорошо знаете настройки безопасности вашей учетной записи в социальной сети. Никогда не полагайтесь на настройки «по умолчанию», самостоятельно настройте их и регулярно проверяйте, поскольку сервисы могут меняться.
- Будьте осторожны, когда устанавливаете приложения, которые рекомендуют социальные сети. Используйте эти приложения, только если вы доверяете источнику, вы должны понимать, какую информацию они будут выставлять напоказ и иметь возможность контролировать ее поток
  (для дополнительной информации о безопасности паролей см. https://security.ngoinabox.org/en/chapter-10).

6. Безопасность мобильной телефонной связи
- В настоящий момент настройки и технологии в области мобильной связи небезопасны (включая СМС и голосовые звонки). Ваше местоположение может быть отслежено и ваши разговоры записаны, поэтому всегда старайтесь использовать более безопасный способ для передачи важной информации.
- Самые безопасные мобильные телефоны – это дешевые незарегистрированные телефоны с предоплаченным тарифом связи, которые вы можете уничтожить после использования.
- Активируйте ввод пароля или PIN-кода на вашем мобильном телефоне.
- Не храните особо секретную информацию на вашем телефоне или храните ее в зашифрованном виде.
- Постоянно будьте осторожны в отношении вашего окружения, когда используете мобильный телефон, и старайтесь не использовать его в опасных местах и ситуациях.
- Убедитесь, что вся ваша информация удалена с мобильного телефона, прежде чем продавать его или сдавать в ремонт.
- Уничтожайте неиспользуемые телефоны и старые SIM-карты прежде, чем выбрасывать их.
- Когда работаете с людьми или организациями, которым направляете особо секретную информацию, старайтесь использовать отдельные телефоны и SIM-карты для работы и личного использования
  (для дополнительной информации о безопасности паролей см. https://security.ngoinabox.org/en/chapter-9).