# ЦИФРОВАЯ БЕЗОПАСНОСТЬ
(РУКОВОДСТВО ДЛЯ ЖУРНАЛИСТОВ)

Душанбе
2015

ББК 76-12 (2 тадж)
Ц 75

**Под общей редакцией**
Нуриддина КАРШИБОЕВА,
председателя НАНСМИТ

**Составители:** Абдуфаттох Вохидов, Нодира Рахмонбердиева, Сухроб Пулотов
**Правовой консультант**: Сухроб Пулотов

**Цифровая безопасность** (руководство для журналистов), Душанбе, 2015, стр**.**

Настоящее руководство издано Национальной ассоциацией независимых СМИ Таджикистана (НАНСМИТ) в рамках проекта «Цифровая безопасность для таджикских журналистов», при поддержке International Media Support (Дания). Распространяется бесплатно.

Руководство подготовлено на основе материалов международных журналистских и правозащитных организаций, опубликованных в Интернете. Они были обобщены, систематизированы и адаптированы с учетом условий Таджикистана. Руководство не является абсолютным в положениях, ибо развитие информационно-коммуникационных технологий в мире способствует появлению новых вызовов в сфере информационной безопасности.

Данная публикация носит рекомендательный характер для журналистов и юристов СМИ.

## Предисловие

Мы живем в веке информационно-коммуникационной технологии. Интерактивные электронные издания и новые формы коммуникации производителей контента с потребителями, отличающиеся от традиционных, также любая медиа продукция, являющаяся интерактивной и распространяемая цифровыми методами относятся к новым медиа. С развитием новых медиа все более актуальной становятся проблемы цифровой безопасности, ибо развитие цифровых, сетевых технологий и коммуникаций наряду с положительными изменениями в информационном пространстве также имеет ряд опасностей.

«Цифровая безопасность» представляет собой сочетание инструментов и привычек, которые пользователи могут использовать, во избежание контроля над их действиями в Интернете, доступа или вмешательства в их электронную информацию и вмешательства в их электронные устройства и программы.

Новые технологии могут представлять опасность для журналистов, если они не

будут использоваться с осторожностью. Репортеры, освещающие вопросы прав человека, журналисты-расследователи, которые привлекают общественное и международное внимание к преступлениям и правонарушениям, подвергаются особому риску.

Международный опыт свидетельствует, что несколько репрессивных правительств и могущественных корпораций использовали современные технологии наблюдения, чтобы разыскать журналистов (как профессиональных, так и цивильных граждан), и наказать их за работу. Если журналисты не будут осторожны, "заметая следы" при работе в сети, кто угодно, имея несколько основных хакерских навыков, может проследить шаги журналиста, подвергая опасности как репортера и его/ее источники. Последние вызовы в сфере СМИ Таджикистана также показывают, что взлом электронной почты и аккаунты журналистов и активистов гражданского общества в социальной сети, прослушивание телефонных разговоров и другие виды киберпреступлений становятся традиционными в борьбе со свободой слова и

информации. Опасность, также проявляется в виде краж личных данных пользователей цифровых технологий (личные данные, документы) и физическое обнаружение человека (геолокация, IP адреса и т.п.).

Настоящее руководство для журналистов призвано не играть в «шпионы», а позаботиться о безопасности профессиональной деятельности и своих источников информации. Вместе с тем, пользуясь новыми медиа, мы не должны допускать такие технические риски как, кражу и подбор паролей, персональных данных, распознавание IP-адреса и установление личности, кражу данных с компьютера пользователей и др.

Никакой набор мер предосторожности и советы не могут полностью гарантировать вашу безопасность и безопасность ваших данных, но следование основным принципам цифровой безопасности может помочь сохранить вашу безопасность и безопасность ваших источников.

# I. ОБЩИЕ ВОПРОСЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ

## Информационная безопасность

Информационная безопасность предполагает обеспечение защиты всей вашей информации - от исследовательских заметок до конфиденциальных данных о ваших контактах и от основных пунктов вашего маршрута до аудио- и видеофайлов. Речь идет как о защите данных, которые вы считаете важной информацией, так и об обеспечении безопасности коммуникаций с вашими коллегами или источниками. Если вы откомандированы для выполнения редакционного задания, то файлы, хранящиеся в памяти вашего компьютера, являются самым ценным вашим достоянием. Их потеря может сорвать подготовку репортажа или, что еще хуже, подвергнуть вас или ваши источники опасности.

## Насколько велики масштабы цифровой безопасности?

Масштабы и изощренность хакерских атак на журналистские цифровые данные

нарастают устрашающими темпами. Компьютеры журналистов подвергаются заражению шпионскими вирусными программами, замаскированными под приложения по электронной почте. Власти прослушивают телефонные переговоры журналистов и просматривают их электронную почту и SMS-сообщения. Слежку с использованием цифровых устройств и помехи в работе журналистов организуют не только государственные структуры, но и крупные криминальные группировки, которые все чаще и чаще используют новейшие технологические достижения.

Меркантильные или «патриотически» настроенные компьютерные агрессоры также «выцеливают» журналистов, работающих с ценной или противоречивой информацией.

В конечном счете, однако, обеспечение высокой степени информационной безопасности не сводится лишь к отражению искусных DDoS-атак или борьбе с хакерами «голливудского типа». Оно предполагает понимание мотивов и возможностей тех, кто мог бы атаковать ваш

компьютер, и выработку стойких навыков, основанных на соответствующих оценках.

**Осознаете ли угрозы?**

Информационная безопасность ставит перед людьми трудно решаемые проблемы. Например, то, что ваш компьютер атакован, заметить достаточно сложно. Если кто-то успешно скопировал ваш жесткий диск (например, отсканировав его, пока вы сидели в соседней комнате), вы вообще можете об этом не узнать. Во-вторых, ущерб, полученный в результате утечки ваших персональных данных, обычно невозможно возместить. Если ваша информация стала известна тем, кто атаковал ваш компьютер, вернуть ее вам не удастся. Наконец, информационно-технологические системы чрезвычайно сложны и постоянно совершенствуются. Даже самый высококлассный программист может не знать назначения той или иной компьютерной программы или того, как можно использовать взаимодействие этой программы с Интернет-сайтами в чьих-либо интересах.

**Можно ли полагаться на интуитивное понимание?**

В вопросе же обеспечения компьютерной безопасности на интуитивное понимание можно полагаться в значительно меньшей степени. Что это значит? Организуйте все как можно проще. Нет смысла иметь систему компьютерной безопасности, которой вы не будете пользоваться, или ту, что не обратит внимания на слабое звено где-нибудь на другом конце цепи. Полагайтесь на то, что вам хорошо известно: от кого можно ожидать компьютерной атаки или создания иных помех вашей работе; какие цели эти люди преследуют или чему они хотят помешать. Используйте эти знания для того, чтобы определить, что именно - и как - вам следует защищать.

**Как быть защищенным?**

Спросите себя: какую информацию мне нужно защитить? Какие данные представляют ценность для меня или для потенциального противника? Возможно, ответить на эти вопросы вы сможете не

сразу. Многие журналисты полагают, что их работа, в общем - прозрачна, и что им нечего скрывать. Однако задумайтесь о том, какой вред вы можете нанести своим источникам, если сообщенная ими вам информация станет известна более широкому кругу лиц. То, что представляется вам безобидной частной информацией, может оказаться поводом для уголовного преследования других людей. Даже информация, которой вы когда-то свободно обменивались с кем-либо в Интернете, может скомпро-метировать вас в ином контексте. Удалить уже опубликованную информацию трудно, но может быть, вам следует «подчистить» свои страницы в Facebook'е или других социальных сетях, либо дополнительно защитить свои персональные данные перед путешествием или командировкой для выполнения нового задания.

**Что означает информационная безопасность?**

Информационная безопасность - это защищенность информации и поддер-

живающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. Природа этих воздействий может быть самой разнообразной.

Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, и стихийные бедствия (землетрясение, ураган, пожар) и т. п.

Информационная безопасность компьютерных систем достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы.

**Что такое конфиденциальность данных?**

Конфиденциальность данных - это статус, предоставленный данным и определяющий требуемую степень их

защиты. К конфиденциальным данным можно отнести, например: личную информацию пользователей; учетные записи (имена и пароли); данные о кредитных картах; данные о разработках и различные внутренние документы; бухгалтерские сведения. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

**Что такое целостность информации?**

Под целостность информации понимается свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, то есть если не произошло их случайного или преднамеренного искажения или разрушения.

Обеспечение целостности данных является одной из сложных задач защиты информации.

**Что такое достоверность информации?**

Достоверность информации – свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

**Что означает защита информации в цифровом пространстве?**

**Защита информации** - это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую инфор-мацию.

**Объект защиты** - информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

**Цель защиты информации** - это желаемый результат защиты информации. Целью защиты информации может быть

предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

**Защита информации от утечки** - деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (далее НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

**Защита информации от разглашения** - деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

**Защита информации от НСД** – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом, с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим НСД к

защищаемой информации, может быть государство, юридическое лицо, группа физических лиц, в т. ч. общественная организация, отдельное физическое лицо.

**Что такое информационные ресурсы?**

Информационные ресурсы - это организованная совокупность документированной информации, включающая базы данных и знаний, массивы, т.е. отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). К информационным ресурсам относятся печатные, рукописные, электронные издания, которые содержат нормативные и справочные документы по законодательству, политической, социальной сфере, отраслям производства и т.д. Информационные ресурсы могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, орга-

низаций и общественных объединений. Отношения по поводу права собственности на информационные ресурсы регулируются соответствующим гражданским законодательством.

**Что означает доступность информации?**

Доступность информации подразумевает доступность компонента или ресурса компьютерной системы, то есть свойство компонента или ресурса быть доступным для законных субъектов системы. Этими ресурсами и компонентами компьютерной системы могут быть: принтеры; серверы; рабочие станции; данные пользователей; любые критические данные, необходимые для работы.

С каждым субъектом системы (сети) связывают некоторую информацию (число, строку символов), идентифицирующую субъект. Эта информация является идентификатором субъекта системы (сети). Субъект, имеющий зарегистрированный идентификатор, является законным (легальным) субъектом.

**Что означает понятие санкционированный доступ к информации**?

Санкционированный доступ к информации - это доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регла-ментации права доступа к компонентам системы, также доступ к информационному ресурсу, который осуществляется штатными техническими средствами в соответствии с установ-ленными правилами.

**Что такое несанкционированный доступ к информации?**

Несанкционированный доступ - преднамеренное обращение пользователя к данным, доступ к которым ему не разрешен, с целью их чтения, обновления или разрушения, либо доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Несанкционированный доступ может создать любой из видов угроз безопасности информации: утечку/рассекречивание/, нарушение целостности или блокирование.

Лицо или процесс, осуществляющие НСД к информации, являются нарушителями правил разграничения доступа. НСД является наиболее распро-страненным видом компьютерных нарушений.

**Как осуществляется НСД?**

Основными каналами несанкционированного доступа, через которые нарушитель может получить доступ к компонентам автоматизированной системы (далее АС) и осуществить хищение, модификацию и/или разрушение информации являются:

- штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;

- технологические пульты управления;
- линии связи между аппаратными средствами АС;
- побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.

**Наиболее распространенные способы НСД?**

Из всего разнообразия способов и приемов несанкционированного доступа остановимся на следующих распространенных и связанных между собой нарушениях:

- перехват паролей;
- «маскарад»;
- незаконное использование привилегий.

**Перехват паролей** осуществляется специально разработанными программами. При попытке законного пользователя войти в систему программа-перехватчик имитирует на экране дисплея ввод имени и пароля пользователя, которые сразу пересылаются владельцу программы-перехватчика, после

чего на экран выводится сообщение об ошибке и управление возвращается операционной системе. Пользователь предполагает, что допустил ошибку при вводе пароля. Он повторяет ввод и получает доступ в систему. Владелец программы-перехватчика, получивший имя и пароль законного пользователя, может теперь использовать их в своих целях. Существуют и другие способы перехвата паролей.

**«Маскарад»** - это выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями. Целью «маскарада» является приписывание каких-либо действий другому пользователю либо присвоение полномочий и привилегий другого пользователя. Примерами реализации «маскарада» являются:

- вход в систему под именем и паролем другого пользователя (этому «маскараду» предшествует перехват пароля);
- передача сообщений в сети от имени другого пользователя.

«Маскарад» особенно опасен в банковских системах электронных платежей, где неправильная идентификация клиента из-за «маскарада» злоумышленника может привести к большим убыткам законного клиента банка.

**Незаконное использование привилегий.**

Большинство систем защиты устанавливает определенные наборы привилегий для выполнения заданных функций.

Каждый пользователь получает свой набор привилегий: обычные пользователи – минимальный, администраторы - максимальный. Несанкционированный захват привилегий, например посредством «маскарада», приводит к возможности выполнения нарушителем определенных действий в обход системы защиты. Следует отметить, что незаконный захват привилегий возможен либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий.

**Какие наиболее распространенные угрозы безопасности существуют для автоматизированных систем (АС)?**

Искусственными, преднамеренными и активными угрозами безопасности АС, которые наиболее распространены являются «троянский конь» (ее также называют «троянской программой»), «вирусы», «сетевые черви».

**«Троянский конь»** представляет собой программу, которая наряду с действиями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению безопасности системы и деструктивным результатам. Аналогия такой программы с древнегреческим «троянским конем» вполне оправдана, так как в обоих случаях не вызывающая подозрений оболочка таит серьезную угрозу. Радикальный способ защиты от этой угрозы заключается в создании замкнутой среды исполнения программ, которые должны храниться и защищаться от несанкционированного доступа.

**Вирус** (компьютерный) представляет собой своеобразное явление, возникшее в процессе развития компьютерной и информационной техники. Суть этого явления состоит в том, что программы-вирусы обладают рядом свойств, присущих живым организмам, - они рождаются, размножаются и умирают. Термин «вирус» в применении к компьютерам был предложен Фредом Коэном из Университета Южной Калифорнии. Исторически первое определение, данное Ф. Коэном, было следующим: «Компьютерный вирус - это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению».

**Сетевой червь -** разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. В отличие от компьютерных вирусов червь является самостоятельной программой.

Зачастую черви даже безо всякой полезной нагрузки перегружают и временно

выводят из строя сети только за счёт интенсивного распространения.

В случае если на вашем компьютере не установлен антивирус, либо произошла заражение компьютера, несмотря на наличие антивируса, пользователь может проверить свой компьютер используя сервисов он-лайнпроверки на вирусы по сайту http://antivirus-alarm.ru/proverka/

**Возможно ли вычислить злоумышленников и привлечь к ответственности?**

По запросу правоохранительных органов провайдеры должны предоставить все записи что были и по ним можно идентифицировать человека.

**По какому принципу вычисляют Интернет террориста?**

Прежде всего, определяется его IP-адрес, определяется точка выхода в эфир, определяется есть ли камера поблизости либо в помещении где он вышел в интернет (например, в интернет-кафе есть камера, берется записи и путем сверки и сопоставления устанавливается лицо. Также

при использовании пресловутых прокси (анонимайзеры) можно путем корреляции информации (сравнение поисковых информации) установить лицо.

**Выводы и советы:**

**1.** Приобретайте лицензионные программы. Прежде чем приобретать компьютерные программы обращайтесь к рекомендациям специалиста в области компьютерных технологий и информационной безопасности.

2. Установку программ на ваш компьютер и ее обслуживание доверяйте специалисту.

3**.** Выбирайте специалиста-компьютерщика из круга ваших общений, можно по рекомендации ваших коллег, друзей и т.д.

4. Не доверяйте собственных носителей информации посторонним лицам и не давайте им пользоваться в вашей отсутствии.

5. Повышайте свои знания в области информационной безопасности…

## II. ЭЛЕКТРОННЫЕ ПОЧТЫ, ИНТЕРТЕТ И ПОЧТОВЫЕ СЕРВЕРЫ

Работу СМИ невозможно пред-ставить без информационных технологий. Через электронную почту моментально обмениваются документами с коллегами, в то же время в локальных либо глобальных ресурсах (внутренние сети, серверы, интернет и т.д.) размешают информацию различного характера. Эти информации и документы могут быть доступными для широкого круга пользователей или ограниченными, а то и вовсе закрытыми. Ограничения доступа обеспечивается различными способами защиты информации как технического, так и физического характера. Это шифрование, закодирование информации, защита паролем, допуск путем идентификации и аутентификации личности, авторизации и т.п.

**Как создавать и хранить надежные пароли?**

Люди привыкли защищать важную информацию с помощью ключей. Ключ от

квартиры, ключ зажигания в автомобиле, PIN-код банковской карточки, пароль к электронному почтовому ящику, и так далее. Есть ключ - есть доступ. Можно построить сложную систему запоров, задвижек, замков, сейфов, но если все это открывается единственным универсальным ключом, который висит на крючке у входной двери, грош цена такой системе безопасности.

**Каким должен быть хороший пароль?**

Чтобы обеспечить свою информационную безопасность, вам необходимо придумать надежный пароль для работы с компьютером.

По мнению экспертов по кибербезопасности пароли должны быть:

- Достаточно длинным, хотя бы 8-10 символов. Иногда компьютерные программы используют целые парольные фразы.
- Неочевидным. Грубую ошибку совершает тот, кто выбирает в качестве пароля личную информацию, например, номер телефона или кличку любимой собаки. Эти

данные могут быть известны другим людям, а значит, им несложно подобрать пароль. В фильме «Идеальное преступление» весь план главного героя в исполнении Майкла Дугласа развалился в один момент из-за того, что он выбрал для своего личного сейфа пароль - дату собственной свадьбы.

- Уникальным. Не используйте один и тот же пароль снова и снова. В противном случае удачный подбор - и все ваши сайты, дневники, сообщения на форумах достанутся злоумышленнику. Общее правило: каждому ресурсу - свой пароль.
- Обновляемым. Пароль - не надпись на памятнике. Меняйте его время от времени. Случается, что человек так привыкает к паролю, что не хочет с ним расставаться и пароль не меняется месяцы, а то и годы. Чем дольше хранится пароль, тем выше вероятность, что его, в конце концов, узнают те, кому не следовало,
- Приватным. Некоторые наклеивают листочки с паролями на монитор. Наверное, у вас нет этой вредной привычки. Но если пароль все-таки стал известен другим людям (*скомпро-метирован*), смените его как

можно скорее. Не стоит хранить пароли в открытых текстовых файлах, документах Word, словом, в таких «контейнерах», которые с легкостью откроет и прочтет всякий.

Для обеспечения надежности пароля можно пользоваться некоторыми хитростями. Вот несколько примеров:

- Меняйте регистр. Как вам, например, такой пароль: «Семнадцать мгновений весны»? (Каждая первая гласная в слове дана в верхнем регистре).
- Используйте не только буквы и цифры, но и другие значки, например, точки, дефисы. Иногда можно удачно заменить букву цифрой, скажем, так: «30л0тые ябл0ки солнца». Здесь буквы «О» заменены нулями (а буква «З», кстати, цифрой «З»).

**Можно ли скомпрометировать пароль?**

Да, и несколькими способами. Например, можно просто подглядеть, как некто набирает свой пароль на клавиатуре. А можно установить программу-перехватчик,

которая будет отслеживать нажатия на клавиши и передавать эти сведения «хозяину». Бдительный пользователь способен оградить себя от этих бед. Присматривайтесь к тому, что происходит вокруг, регулярно запускайте антишпионские и антивирусные программы, не забывайте их обновлять.

**Защищайте свои персональные данные**

Чтобы подобрать пароль, злоумышленник может задаться целью собрать персональные данные о его владельце. Довольно часто люди выбирают в качестве паролей то, что легко запомнить: год рождения, имя кого-то из членов семьи или друга, место рождения, название любимой футбольной команды и т.д. Злоумышленник аккуратно собирает такие данные. Пароль легко «сдается» злоумышленнику, если у того есть персональные данные его владельца. Сегодня это самый распространенный способ получить доступ к информационной системе (и настойчивые хакеры нередко им пользуются).

**Можно ли доверять незнакомому вам человеку?**

Есть довольно хитрые методы выуживания пароля у человека. Существуют целые сценарии. Телефонный звонок, вы снимаете трубку, и на другом конце провода раздается вежливый голос: «Здравствуйте, это ваш провайдер Интернета. Мы устанавливаем новый сервер и проявляем заботу об информации клиентов. Мы не хотим, чтобы вы потеряли электронную почту. Пожалуйста, напомните, какой у вас пароль?» Или же какой-то тип представляется сотрудником из другого отдела вашей компании: ему нужен пароль для доступа к общему ящику электронной почты. А единственный человек, знающий пароль, увы, тяжело болен, поэтому…

Ни в коем случае не раскрывайте компьютерную информацию (особенно пароли и коды доступа) по телефону, если вы не можете подтвердить личность собеседника.

**Как обезопасить собственный компьютер?**

Используйте все свои знания и опыт, чтобы обеспечить базе данных хорошую защиту. Закройте путь вирусам и хакерам из Интернета на ваш компьютер. Если есть необходимость сделайте резервные копии и надежно их храните, зашифровывайте и спрячьте от посторонних, используйте для этого специальные программы шифраторы, старайтесь, чтобы ваши действия не вызывали подозрения у окружающих.

Известно, что важным средством защиты компьютера является антивирус, но еще важнее принять дополнительные меры предосторожности, если ваше рабочее место или помещение подключено к таким сервисам как E-mail, Twitter, Facebook или Skipe. Социальные сети и средства связи часто являются каналами для распространения вируса.

Не перегружайте ваши файлы ссылками и не щелкайте мышью по ссылкам, которые вам присылают неизвестные отправители.

Тщательно проверяйте адрес электронной почты или аккаунт Twitter тех пользователей, которые выходят на связь с вами. При возникновении сомнений проверяйте личные данные отправителя по другим контактам или с помощью поисковых инструментов.

**Как хранить информацию?**

Даже если вы осторожны с использованием веб-ресурсов и общением с источниками, вам нужно хранить информацию, которую вы получаете где-то, помимо головы. Такое простое действие, как «запись на бумаге», делает информацию чрезвычайно доступной.

Чтобы удостовериться, что информация, которую вы храните, надежно защищена:

- защищайте ваш компьютер и мобильный телефон паролями, которые знаете только вы;
- никогда не разглашайте свои пароли, никуда не записывайте их, кроме как на специальном сервисе для хранения паролей KeePass; также, используйте разные пароли

для разного оборудования и разные пароли для разных веб-ресурсов, электронной почты, Facebook, Twitter и др.;

- никогда не покидайте свой компьютер без присмотра с открытыми важными документами, даже на несколько минут;
- выйдите со своего аккаунта, и убедитесь, что для повторного входа вам необходимо зарегистрироваться;
- не оставляйте технику с важной информацией в кафе, такси, и т.д. Не держите телефон в кармане, или открытой сумке, где он может быть легко вытащен. В дополнение, защитите свой телефон паролем, и блокируйте его после каждого разговора. Если ваш телефон поддерживает буквенные пароли, используйте их вместо простых четырехзначных кодов;
- рассмотрите возможность зашифровки особо важной информации содержащейся на жестком диске или USB, используя различные программы, например TrueCrypt, с помощью которой вы можете хранить свои файлы в электронном «сейфе», доступ к которому совершается через пароль (Не

забудьте этот пароль, иначе вы потеряете доступ к своим данным).

**Как зашифровать и спрятать информацию?**

Попробуем выделить два основных подхода к защите информации. Данные можно зашифровать так, что их не сможет прочесть посторонний человек. Или их можно спрятать, чтобы злоумышленник даже не подозревал о том, что данные существуют. Замечательная программа Truecrypt решает обе задачи сразу.

Мы порою думаем, что наш компьютер защищен паролем, Windows тоже требует пароль, устанавливаем пароли для документов Word, для архивов zip и т.п. Если всерьез заботишься о безопасности, такая защита условная. Любой пользователь, прочитавший книжку об устройстве компьютера или даже инструкцию к материнской плате, сумеет сбросить "пароль при включении". Нужно всего-то открыть корпус и поставить перемычку.

Зашифровать информацию - примерно то же, что и положить в хороший сейф,

только надежнее. Хороший специалист в области информационной безопасности способен взломать вашу защиту. Компьютерные программы (многие из которых бесплатны и доступны широкому кругу людей) умеют создавать такие электронные "сейфы", на вскрытие которых даже у крупных корпораций или спецслужб с их мощными компьютерами, деньгами и специалистами уйдут не часы и даже не дни, а годы. Принцип действия этих программ разные. Рассмотрим одну из таких программ Truecrypt. Она создает на диске компьютера защищенный (зашифрованный) том. Физически это файл, который может называться как угодно (по выбору пользователя). Операционная система Windows "видит" этот файл как отдельный диск. При записи на этот "диск" данные автоматически шифруются. При чтении – расшифровываются. Все происходит "на лету", пользователь работает так, как работал бы с обычным диском.

Возможно, вы имеете дело с большим количеством информации, которую нежелательно разглашать посторонним. В таком

случае есть общее правило: не храните такую информацию по принципу "а пусть будет". Если без нее можно обойтись - удалите.

**Как не вызвать подозрений?**

Бывает, однако, что сам факт использования шифрования способен вызвать нездоровый интерес злоумышленников ("если зашифровано, значит, что-то важное"). Для некоторых людей это является решающим аргументом против шифрования. Давайте не будем ничего менять, говорят они. Меньше подозрений - меньше риска.

Они ошибаются. С одной стороны, работать с серьезными материалами и делать расчет только на то, что удастся не привлечь внимание это не благоразумно. С другой стороны, данные можно не только зашифровать, но и спрятать.

Действительно сам по себе факт использования шифрования может стать поводом для давления и репрессий в отношении обладателя информации.

- Можно вообще отказаться от защиты важной информации. Это просто. Но в

любой момент базы могут быть изъяты, выкрадены.

- Можно использовать стеганографию: скрывать важную информацию в безобидных файлах, например, в картинках. Есть программы, которые умеют это делать. Но стеганография подразумевает ручную работу. Этот метод в большей степени подходит для единовременной передачи какой-то краткой информации по электронной почте.
- Можно хранить всю важную информацию не на своем компьютере, а на удаленном сервере. Тем которым опасается рыска обыска и изъятия компьютерной техники этот вариант приемлемым, но работа с удаленными данными требует аккуратности, четкого понимания происходящих процессов, подключения к Интернету (желательно высокоскоростного, если речь идет о больших объемах данных).
- Можно записывать самую важную информацию на флешку. Но такие устройства едва ли более надежны, чем жесткие диски. В конце концов, флешку нетрудно просто потерять.

Можно переименовать файл Truecrypt, либо изменить ее расширение, например .avi. Он будет выглядеть как видео, скажем, кинофильм, и не вызовет подозрений. Даже если в случае ее обнаружения - нужно убедить их, что они нашли именно то, что искали. Хотя на самом деле вся важная информация будет храниться в другом месте. Truecrypt позволяет создавать "спрятанный" том внутри обычного тома. Никто, кроме вас, не знает, что "спрятанный" том вообще существует. Его невозможно увидеть и даже заподозрить. Поэтому даже если злоумышленникам в руки попадет защищенная Truecrypt информация, даже если они раздобудут пароль, они ни за что не догадаются, что внутри сейфа есть еще одно, маленькое, тайное отделение, где хранится то, что действительно важно.

**Как избежать потери данных?**

Вы можете потерять данные в следствии технического износа носителей, их взлома и приведения в непригодности, действия компьютерных вредителей, либо сетевых атак, кражи информации с вашего

компьютера, преднамеренного либо непреднамеренного удаления вами или другим посторонним пользователем и много другое. Для того чтобы избежать потерю важных информаций, вам необходимо сделать их резервную копию.

**Где создавать и хранить резервные копии?**

Главное правило здесь: резервная копия должна храниться на ином носителе данных, чем оригинал. Местонахождение и условия обращения носителей должны быть такими, чтобы гибель оригинала не означала гибели резервной копии - и наоборот.

- Компакт-диск. На CD "влезает" до 700 Мб данных, в большинстве случаев этого достаточно для регулярного резервного копирования. На DVD - 4.7 Гб. Это удачный выбор, если речь идет о резервных копиях больших объемов данных, например, архивов фото или видео. Современные компьютеры обычно продаются с DVD-RW-приводами, которые позволяют записывать и CD, и DVD. В качестве "болванок" используются более дешевые CD-R, DVR+-

R с возможностью однократной записи или более дорогие CD-RW и DVR-RW - на них можно перезаписывать многократно. Понадобится также программа для записи (иногда говорят "прожига") дисков, такая, как DeepBurner, Nero и многое другое.

- USB-флешка, маленькое устройство, которое подсоединяется к порту USB компьютера (сейчас такими портами оснащены все компьютеры, в том числе ноутбуки). При подключении опознается компьютером как еще один диск, а значит, не требуется специальная программа записи данных - файлы можно переносить на флешку в том же "Проводнике" Windows. Носитель перезаписываемый, емкость измеряется гигабайтами.
- Флеш-карточки, в основном распространенных стандартов SecureDigital, CompactFlash, SonyMemoryStick. Хоть и не столь симпатичны с виду, как USB-флешки, карточки, однако, дешевле, и, что важно, работают не только в компьютерах. Для чтения и записи на карточку требуется "кард-ридер". Спе-циальные программы для записи не нужны.

• Съемные жесткие диски, накопители на магнитной ленте, дискеты Zip и прочие, еще более экзотические варианты.

• Стоящий особняком способ хранения информации - запись через Интернет на удаленный сервер. Возможно, единственный реальный вариант спасения важных данных в условиях давления на организацию, репрессий в отношении активистов, обысков, изъятия компьютерной техники и т.д.

**Как это автоматизировать**?

Для создания резервных копий на регулярной продолжительной основе разработаны программы, которые позволят автоматически сохранять ваши данные. Например, не нужно ломать голову над тем, где расположены почтовые папки, адресная книга, закладки, настройки браузера и др. Небольшая удобная программа MozBackup быстро создаст полную или частичную (по вашему выбору) копию этой информации.

А программа CobianBackup позволяет не просто создавать резервные копии важных файлов, но и делать это по расписанию, переносить на удаленный

сервер, сжимать и шифровать. Программа может запускаться сама, периодически, в установленное вами время, и работать в фоновом режиме, не отвлекая вас вопросами. Если вам требуется скопировать большой объем данных, программа может заняться этим, когда вы уйдете с работы, а по завершении сама выключит компьютер.

Маленькая программа AllwaySync позволит синхронизировать содержимое двух носителей (например, папки на жестком диске с оригиналом данных и папки на флешке с резервной копией данных).

- Привести в порядок файлы и папки на компьютере. Избегать ситуаций, когда файлы в рамках одной работы оказываются "в разных углах" жесткого диска.
- Не реже раза в неделю делать полное резервное копирование всех данных из уже составленного "важного списка" (автоматически). Записывать эти данные на DVD-диски.
- Хранить эти DVD-диски за пределами офиса в надежном месте.
- Часть информации сохранять на удаленном сервере в Интернете и обяза-

тельно защищать ее с помощью шифрования (конечно, тоже автоматически).

- Дистрибутивы программ, серийные номера и прочую важную информацию, доступную только в печатном виде, хранить на отдельной полке в запирающемся шкафу.

Аккуратность и четкое следование однажды принятым правилам создания резервных копий - лучшая страховка на случай любых потерь информации.

**Как восстановить случайно потерянные файлы?**

Восстановление удаленных файлов или данных с поврежденных жестких дисков и других накопителей - задача, с которой хотя бы однажды сталкивается почти каждый пользователь. Если при работе с файлами вы случайно их удалили (из корзины тоже), либо отформатировали жесткий диск, то не расстраивайтесь, их можно восстановить. Хотя восстановление данных с жесткого диска, флешек и карт памяти — дорогая и, к сожалению, иногда востребованная услуга. Однако во многих случаях, вполне можно попробовать бесплатную

программу, чтобы восстановить важные данные. При грамотном подходе, это не повлечет за собой дальнейшее усложнение процесса восстановления, а потому, если у Вас не получится, то специализированные фирмы все так же смогут вам помочь. Для этого есть очень много и платных и безвозмездных программ, к примеру, HandyRecovery, R-studio, Recovery Software, PowerData Recovery, Seagate File Recovery for Windows и другие.

Эти программы предназначены для восстановления файлов случайно удаленных с жесткого диска или других носителей информации. Они также могут восстанавливать файлы поврежденные в результате вирусных атак, перебоев энергоснабжения и сбоев программного обеспечения, файлы с удаленных и отформатированных патриций. Если какая-то программа не использует Корзину во время удаления файлов, HandyRecovery может восстановить и такие файлы. Она также может восстановить файлы из Корзины после ее очистки.

Также можно воспользоваться программой Recuva, которая помогает поль-

зователям восстанавливать удаленную информацию.

**Как надежно стереть отдельный файл?**

У большинства людей есть некоторые данные, которыми бы они не пожелали делиться с другими – пароли, персональные данные, секретные документы с работы, финансовые отчёты, художественные произведения, список можно продолжать.

Возможно, вы храните часть этой информации на вашем компьютере, где это удобно для быстрого доступа, но когда приходит время для удаления данных с жёсткого диска, всё становится немного сложнее, и обеспечение конфиденциальности не так просто, как может показаться на первый взгляд.

Ваша первая мысль, что когда вы "удаляете файл", то данных больше нет? Это совсем не так! Когда вы удаляете файл, операционная система не по настоящему удаляет файл с диска, она лишь удаляет указатель файла из таблицы файловой системы, т.е. если вы стерли файл в

Windows, он как бы перемещается в "Корзину". Восстановить его оттуда не представляет труда даже для начи-нающего пользователя. Windows не стирает файл в буквальном смысле этого слова. Опера-ционная система только помечает файл как удаленный. Информация остается на диске, пока Windows не понадобится место, чтобы записать что-то другое. "Вторая жизнь" файла может длиться часы, дни, недели. Файл остаётся на диске до тех пор, пока другой файл не создастся на его месте, и даже после этого есть возможность восстановить данные, изучая магнитные поля на поверхности диска.

Прежде чем файл будет перезаписан, любой человек легко может получить к нему доступ при помощи специализированных программ восстановления данных и пол-ностью или частично восстановить файл.

Есть несколько проблем в безопасном удалении файлов, по большей части вызванных использованием кэширования записи, конструкцией жёсткого диска, и использованием шифрования данных.

Чтобы наверняка избавиться от ненужных копий своей базы данных вам потребуется нечто более совершенное, чем стандартная "Корзина" Windows.

В операционной системе Windows имеется и такая функция, которая удаляет файлы не размещая в корзину. Для этого одновременно с пунктом удаления необходимо нажать кнопку Shift. В случае обращения к такой функции будьте внимательны и осторожны, так как после удаления файла вы сами не можете без специальных вышеупомянутых программ восстановить удаленный файл.

Есть и другой вариант, надо внести изменения в контекст файла (можно удалить весь текст) с последующим ее сохранением с учетом изменений. Данный вариант применим к тем файлам, которые носят текстовое содержание.

Следующий инструмент это специальные программы удаления файлов и очистки жесткого диска компьютера как Eraser, Unlocker, File ASSASSIN, Lock Hunter, IObit Unlocker и множество других программ, которые позволяют полностью

удалить персональные данные с жёсткого диска путём многократной перезаписи тщательно выбранными методами.

**Как нужно стереть без следа данных на носителях информации?**

Один из таких инструментов называется Eraser. Это небольшая программа, которая позволяет "начисто" удалять файлы с диска. Программа "дружит" с "Проводником" Windows и другими файловыми менеджерами. Достаточно щелкнуть по файлу правой кнопкой мыши и выбрать в появившемся меню пункт "Очистить". Файл будет многократно переписан случайными данными по специальному алгоритму. Очень полезно очищать неиспользуемое пространство время от времени. Так как, Windows не удаляет файлы буквально, а лишь помечает соответствующую область на диске как свободную (неиспользуемую). Очень скоро "свободное" дисковое пространство заполняется "навидимой" информацией. Не исключено, что среди этой информации есть важные данные, которые следовало бы удалить "начисто".

**Что такое ненужные данные и как от них избавиться?**

В "темных углах" операционной системы Windows могут скрываться данные, которые аккуратному пользователю, вероятно, хотелось бы удалить начисто. Эти файлы не были стерты самой Windows, их не всегда просто обнаружить на диске, поэтому Eraser нам здесь не помощник. Что представляют из себя эти данные? Это:

- Временные файлы Интернета (текст, картинки, всяческие персональные данные, список посещенных сайтов).
- Временные файлы, которые появляются из-за работы разных прикладных программ, например, рабочие копии документов.
- Разнообразные ярлыки, создаваемые Windows для удобства работы.
- Файл подкачки Windows. Файлы подкачки это файлы сохраненные программой Windows вне пределах карты памяти (обычно происходит при переполнении карты памяти), т.е. на самом жестком диске компьютера. Windows при работе "подкачивает" нужную информацию из

этого файла. Это могут быть фактически любые данные. Веб-страницы, текстовые документы, электронные таблицы. Даже пароли. Когда ты выключаешь компьютер, вся информация из памяти исчезает. А файл подкачки остается.

Чтобы удалять вышеуказанные файлы, разработаны специальные программы как CCleaner. Подобно Eraser, он может быстро и надежно вычистить все эти данные, и компьютер станет меньше похож на склад старьевщика.

**Каким образом можно обеспечить безопасность в виртуальном пространстве?**

Для обеспечения безопасности, необходимо предпринимать комплекс технических, инфраструктурных и законодательных мер, которые могут обеспечить эффективное обнаружение кибер атак и противодействие им.

На наш взгляд, противодействие кибератакам можно осуществить с учетом реальных ситуаций. Вот некоторые советы:

• законодательные и инфраструктурные риски кибербезопасности журналиста при работе в Сети зависят от усилий (лоббирование и эдвокаси) всего гражданского сообщества;

• проведение эффективных кампаний по обходу блокировок может минимизировать попытки ограничение доступа к интернет-ресурсам;

• личная техническая безопасность должна быть приоритетом в деятельности журналиста;

• необходимо повышение потенциала создателей контента в сфере их информационной безопасности.

Наряду с вышесказанным при работе в Интернете:

• не открывать входящие сообщения и приложения, в которых нет адреса отправителя или они вам не знакомы, или же если нет темы.

• даже если отправитель вам знаком, то посмотрите, что он вам отправил, если там, например, прикреплен файл «Заработай_1000_баксов.doc», то это скорее всего вирус, которым заразился известный вам

адресат и который рассылает письмо всем адресатам из его адресной книги. Поэтому, прежде чем открывать его, свяжитесь с ним и установите подлинность этого письма.

- вирусы, в основном, содержатся в архивах, поэтому прежде чем распаковывать архивы обязательно проверяйте их на вирусы.

**Целевая атака – что делать?**

Программы-антивирусы, хранители паролей и HTTPS не помогут вам в случае целевой атаки. Если вы стали объектом целевой атаки, скорее всего, вы получили либо e-mail, либо SMS-сообщения Facebook с присоединенными файлом или линком, часто – от людей, которых вы знаете, или чей е-мейл выглядит знакомым. Если вы откроете вложение или пройдете по ссылке в таком письме, вы загрузите на свой компьютер шпионскую программу, которая будет копировать содержимое вашего жесткого диска и отправлять информацию авторам программы. Причем, файл не обязательно будет выглядеть как программа, и иметь расширении exe, он может быть

«замаскирован» под pdf, doc или страницу html.

Чем сложнее и профессиональнее шпионская программа, тем сложнее определить, есть ли она на вашем компьютере. Элементарные программы будут тормозить работу компьютера, включать-выключать веб-камеру, некорректно завершать работу компьютера. Избавиться от такой программы можно переустановив систему, однако следует быть очень осторожным с восстановлением ваших файлов, поскольку восстановив инфицированный файл, вы запустите шпиона снова. Если вы приблизительно знаете, когда вы получили подозрительное письмо, и когда программа была установлена, не восстанавливайте файлы, созданные или загруженные после этой даты. Если же не знаете – не восстанавливайте вообще. В любом случае, если у вас есть подозрения, что вы стали объектом целевой атаки, лучше всего обратиться к специалисту по цифровой безопасности.

Самое простое, что вы можете сделать – это не открывать письма, отправленные с

подозрительных или странных адресов, и уж точно – не открывать присоединенные файлы, как бы привлекательно или безобидно они не выглядели.

**Какими правилами пользоваться для физической защиты информации?**

- Разузнайте побольше о соседях. Кто занимает офисные помещения справа и слева, напротив, этажами выше и ниже? Если в ваше отсутствие в офис начнет ломиться незнакомец, объясняя, что "забыл ключ", можно ли рассчитывать, что сосед снимет трубку и наберет ваш номер? Или соседу все равно? Или он сам - возможная угроза?
- Постарайтесь защитить двери и окна. Как минимум, поставьте приличный замок.
- Отделите приемную, куда приходят люди, от рабочих помещений. Исключите ситуацию, когда посетитель пробирается к вам мимо рабочих мест, заваленных важными документами.
- Установите, кто может брать ключи от офиса, а кто не может. Уладьте вопросы с

уборщицей, если она приходит по вечерам после работы.

- Избегайте ставить оборудование вблизи проходов, где его могут случайно задеть. Компьютерные провода не должны путаться под ногами или свисать гирляндами со столов. Лучше всего убрать провод в специальный короб.
- Выясните у электрика, есть ли в розетках заземление. Если оно есть, используйте его (вилки с тремя контактами вместо двух).
- Проводка и в особенности розетки должны быть качественными. При необходимости замените их.
- Подключите компьютеры к электрической сети не напрямую, а через источники бесперебойного питания (ИБП). Тогда броски напряжения в сети не приведут к выключению и порче компьютеров.
- Если в организации используется беспроводная связь с Интернетом, убедитесь, что для нее обеспечен соответствующий уровень защиты. Посторонний человек не должен иметь возможность подключиться к вашей сети.

• Ставьте компьютер так, чтобы информация на экране не бросалась в глаза людям, проходящим мимо.

• Не забывайте про вентиляцию. В жару компьютер может перегреться. Не придвигайте корпус задней стороной вплотную к стене, не устанавливайте его под прямыми солнечными лучами или у батареи отопления.

• Если у вас есть ноутбук ис-пользуйте специальный замок KensingtonLock. Это запирающее устройство с металлическим тросом, напоминает защиту от угона велосипедов. Ведь ноутбук относительно несложно украсть, воспользовавшись шумной, напряженной офисной обстановкой.

• Отлучаясь ненадолго, не оставляйте на экране компьютера важную информацию. Как минимум, запускайте "заставку Windows" под паролем.

• Не выпускайте из виду мобильные устройства, в частности, ноутбук и мобильные телефоны, особенно во время поездок и остановок в гостиницах. Старайтесь не демонстрировать такие устройства на пуб-

лике, чтобы ненароком не привлечь внимание вора.

- Где бы вы ни были, не забывайте флешки в USB-разъемах компьютеров. Как только работа с флешкой закончена, вытащите ее из гнезда и уберите в надежное место.
- Проведите инвентаризацию оборудования. Если что-то пропадет, не придется спорить, было такое устройство у вас в офисе или нет. Не забудьте про технику, принадлежащую организации, которая находится "на домах" у сотрудников.
- Упорядочите процедуру создания резервных копий самых важных данных: кто, как и когда этим занимается, где хранятся архивы CD и DVD.
- Установите пароль для доступа к компьютеру в BIOS (пароль при загрузке компьютера). Это не станет преградой для изощренного вора, но помешает кому-либо "быстренько" получить доступ к содержимому диска, перезагрузив компьютер.
- Используйте шифрование для защиты информации не только на

настольных компьютерах, но и на мобильных носителях и устройствах.

**Что такое фишинг?**

Фишингом называют совокупность приемов, с помощью которых злоумышленники пытаются выманить у вас ценную информацию. Например, на ваш адрес электронной почты могут прислать письмо якобы от Skype, в котором вам предложат перейти по ссылке для входа в вашу учетную запись и проверки состояния счета.

Щелкнув по этой ссылке, вы попадете на веб-сайт, внешне похожий на сайт Skype, но на самом деле принадлежащий другим лицам. Если вы введете свой логин Skype и пароль, эти люди запишут их в свою базу данных, чтобы впоследствии использовать в своих интересах.

**Как защититься от фишинга?**

Бдительность. Несмотря на то, что эффективность антиспамовых и других защитных фильтров неуклонно повышается, какая-то часть ненужных и вредоносных сообщений все равно минует эти фильтры.

Однако проявляя осторожность и бдительность при ответе на такие сообщения или при попадании на веб-сайты злоумышленников, вы в большинстве случаев сможете предотвратить возможный ущерб.

Сообщения, создающие ощущение неотложности – например такие, как "Если вы не перейдете по этой ссылке, ваша учетная запись Skype будет удалена" или "Ваша учетная запись в опасности! Для получения подробной информации щелкните здесь", – побуждают получателя действовать необдуманно, не проверив источник полученной информации.

Если в сообщении вам предлагают выполнить какое-либо действие со своей учетной записью, не переходите по ссылкам в таком письме, а вместо этого введите skype.com в адресном поле своего веб-браузера и войдите в свою учетную запись непосредственно с веб-сайта Skype.

Если вы оказались на каком-либо веб-сайте через ссылку или другой механизм переадресации, убедитесь, что URL-адрес сайта skype.com и что в этом адресе отсутствуют другие символы или слова.

Например, не стоит доверять веб-сайтам notskype.com и skype1.com.

И помните: если у вас возникли даже малейшие подозрения о том, что ваша учетная запись стала жертвой компьютерных взломщиков или других злоумышленников, не откладывая, зайдите на веб-сайт skype.com и смените свой пароль.

**Как защитить информацию о вашем Интернет-серфинге?**

Один из способов слежки за журналистом – это отслеживание его Интернет-траффика. Заходя на любой интернет-сайт, вы оставляете там «следы» - ваш IP-адрес. Эта информация доступна собственникам и администраторам сайта, всем членам вашей сети, а также вашему Интернет-провайдеру. А значит, по требованию или настойчивой просьбе информация может быть доступна и любым госорганам. Чтобы защитить информацию о вашем Интернет-серфинге, следует пользоваться расшире-нием для браузера HTTPS Everywhere, разра-ботанным Electronic Frontier Foundation и доступным на их веб-

сайте. Это расширение работает с браузерами Firefox, Chrome, Opera и кодирует информацию о вашем Интернет-траффике.

Тем не менее, существуют сайты, которые не поддерживают режим безопасного серфинга, как например LiveJournal. Это не значит, что посещать такие сайты нельзя, однако не стоит оставлять на таких сайтах никакой личной либо уязвимой информации, например в личных сообщениях или «подзамочных» постах.

**Как скрыть Интернет-переписку от посторонних?**

Можно ли положиться на Интернет в смысле безопасности? Увы, нет. Электронное сообщение не так уж трудно перехватить, уничтожить, подделать. Многие люди это умеют. Там, где это возможно, лучше использовать защищенную связь.

Как бы ни передавалась информация - по электронной почте, ICQ или как-то еще - нужно, чтобы отправитель был уверен, что его сообщение дойдет в целости и сохранности и будет прочитано именно тем, кому оно в самом деле было адресовано. А

получатель должен быть уверен, что письмо действительно отправлено вами.

**Как обезопасить свою работу на компьютере с общим доступом?**

Если вы работаете в Интернет-кафе, на компьютере, не принадлежащем вам, старайтесь не оставлять следы по окончанию вашей работы:

- если вы проверяете ваш почтовый ящик, ваш аккаунт в Facebook или ваш аккаунт в Twitter, не забывайте затем отключаться;
- удаляйте историю вашего поиска в браузере. Там содержится обширная информация, которая может быть использована специалистом, в частности, для получения доступа к вашим аккаунтам в режиме онлайн;
- на компьютере с общим доступом никогда не сохраняйте ваш пароль в браузере. Если вы случайно сделали это, постарайтесь удалить его из памяти браузера по окончании работы;
- очищайте поля строк ввода в формулярах;

- удаляйте файлы cookies;
- удаление этих данных в каждом браузере производится различным способом. Удобным средством для предотвращения подобных ошибок является использование «личного браузера» Firefox или Chrome;
- контролируйте доступ к вашим данным.

Большая часть сервисов, работающий в режиме онлайн (Twitter, Facebook, WordPress, Tumblr, Skype и др.) позволяет сохранять забытый пароль благодаря отправке пароля вам по электронной почте. Поэтому важно защищать ваш почтовый ящик как можно надежнее. Если он подвергается опасности, то часто открывается доступ также и к вашим закодированным личным данным.

Почтовый сервис Google, Gmail, позволяет использовать дополнительные средства безопасности: «провернув в два этапа». Этот сервис позволяет защитить вашу электронную почту с помощью: имени пользователя, пароля и кода, который вы получаете на ваш мобильный телефон

каждый раз, когда вы открываете ваш почтовый ящик.

Таким образом, без помощи вашего мобильного телефона невозможно получить доступ к вашей почте.

Когда вы открываете ваш почтовый ящик Gmail, щелкните мышью на позиции «подробности», в нижней части страницы. Это приведет к открытию окна, в котором указывается перечень недавних подключений к вашему почтовому ящику. Таким образом, вы обнаружите подозрительные действия.

Twitter и Facebook также предлагают аналогичные услуги, позволяя вам проверять пакеты приложений и сайты, на которых разрешен доступ к вашей учетной записи.

**Как обеспечить анонимность ваших источников?**

Публикуя статью, либо вы, либо ваш источник может захотеть остаться анонимным. Защита анонимности ваших источников на данном этапе опирается на базовые навыки журналистики. Вы также можете опубликовать статью он-лайн, не раскрывая

свою личность, в виде блога, анонимно. GlobalVoices подготовил пошаговое руководство, которое научит вас, как это сделать.

Основные шаги включают:

1. Зайдите на страничку TorProject.org. Прочитайте руководство перед загрузкой.

2. Загрузите и установите подходящую для вашей операционной системы программу Tor Browser Bundle и используйте его для поиска информации в веб сети, скрывая ваш IP адрес. Вы также можете пользоваться этой программой через USB, если вы пользуетесь общим компьютером.

3. Создайте новый электронный адрес, который трудно проследить, который не содержит личной информации, не связан с вашими другими аккаунтами и мобильным телефоном.

4. Запустите программу Tor, и когда браузер открывается автома-тически (когда Tor начнет работать), создайте новый WordPress блог, зарегистри-рованный под вашим новым анонимным электронным адресом.

5. Пишите свои статьи не в режиме онлайн. Когда вы готовы опубликоваться.

6. Зайдите на ваш новый блог, отредактируйте временные метки, и опубликуйте статью.

7. Для безопасности удалите черновики, историю загрузок, пароли из вашего браузера.

8. При каждой публикации повторяйте шаги 4 – 6.

**Как можно стирать информацию, которую вложили в интернет?**

**Н**икак, разве что обновив информацию (т.е. заменив старую на новый, естественно вымышленный, неправильный)

**Выводы и советы:**

- Используйте разные сложные пароли к доступу на разные ресурсы.
- Не свяжите между собой различные ресурсы.
- Блокируйте доступ к вашим компьютерам и гаджетам с помощью паролей и экранов блокировок;
- Как можно больше храните информации он-лайн под псевдонимом.

- Развивайте свои знания в сфере кибербезопасности. Будьте осторожны, если вынуждены пользоваться своим аккаунтом с чужого компьютера. Не забывайте очищать историю и кеш браузера и удалять сохраненный им пароль.
- По возможности используйте защищенный (SSL) доступ (https://...). Таким образом, можно шифровать сеансы связи между вашим браузером и сетью.

## III. АНОНИМАЙЗЕРЫ, ПРОКСИ-СЕРВЕРА И СОЦИАЛЬНЫЕ СЕТИ

**Что такое анонимайзер?**

Анонимайзер (cgiproxy) – это специальный сайт в интернете, при помощи которого вы можете бродить по интернету без опасения, что будет идентифицирован ваш АйРи (IP) и прочие данные.

**Как работает анонимайзер?**

Вы просто заходите на сайт с webproxy, наберите в строке запроса нужный Вам URL, и нажмите кнопку "Go" (эта процедура очень похожа на поиск в поисковых системах). После этого откроется страница запрошенного Вами сайта, но адресом ее будет адрес CGI proxy.

**Список анимайзеров и немного информации о некоторых из них:**

- http://anonymouse.ws/ - может не только анонимно просматривать страницы, но также отправлять анонимные сообщения по почте и смотреть новости.

- http://www.hidemyass.com/- бесплатный анонимный сервис анонимайзера, который действительно помогает скрыть Ваш реальный IP адрес!
- http://www.shadowsurf.com/ - приватный и 100% анонимный серфинг по интернету с помощью Shadow Surf прокси. Вы можете получить доступ к заблокированным сайтам, при этом Ваш IP адрес будет не виден. Не требует установки программ.
- www.proxyforall.com
- http://easysecurity4u.com/
- http://nu3ga.com/

Остальные:

- http://www.covertbrowsing.com./
- http://www.guardster.com/ - неплохой webproxy. Может разрешать/запрещать cookies, скрипты, рекламу, картинки и рефереры. Нужно набрать адрес под надписью "Free Anonymous Surfing". После этого предлагается принять условия использования сервиса, после чего Вы переходите на нужную страницу. На панели сверху есть красные и зеленые кнопочки, которые

щелчком мыши переключаются между состояниями on и off.

- http://www.proxyweb.net/ - этот анонимайзер может удалять Java, JavaScript, cookies и ActiveX. Кроме того, он использует HTTPS (защищенное соединение), поэтому никто не сможет определить какие файлы Вы скачиваете.
- http://webwarper.net/ - этот анонимайзер умеет сжимать файлы на лету, весьма популярный webproxy. Имеется также русская версия этого cgiproxy сервера. Анонимность, обеспечиваемая WebWarper, неполная: в некоторых ситуациях владельцы сайта смогут определить ваш IP-адрес. Подробнее об этом читайте на сайте WebWarper.
- https://www.megaproxy.com/ и http://www. amegaproxy.com/ - этот анонимайзер может работать с защищенными сайтами (HTTPS), повышая тем самым Вашу анонимность. Зеркало
- http://www.w3privacy.com/ - бесплатный анонимайзер, может удалять cookies, java скрипты, рекламу.

- http://www.anonymizer.ru/ - русский анонимайзер. Этот CGI proxy имеет много дополнительных настроек, доступных после регистрации.
- http://www.the-cloak.com/ - поддерживает HTTP, HTTPS, FTP аноним-ные соединения. Может удалять cookie, scripts и "прятать" рефереры - откуда пришел посетитель.
- http://proxify.com/ - хороший быстрый анонимайзер, который может удалять cookies, рекламу, рефереры, а также использовать HTTPS (защищенные) соединения.
- http://www.snoopblocker.com/ - хороший анонимайзер. Использует 128-битное SSL-шифрование трафика. Позволяет разрешить/заблокировать Java, JavaScript, Cookies, ActiveX.
- http://www.livreproxy.com/ - скрывает Ваш IP от чужих глаз и "пробивает" фильтры в школах и на работе с помощью CGI или PHP прокси.

**Как сохранить анонимность и обойти цензуру?**

Во многих странах мира вполне официально, на государственном уровне существуют системы онлайновых фильтров. Жители этих стран лишены возможности просматривать определенные веб-сайты. Компании, школы, публичные библиотеки также часто используют фильтры для защиты своих сотрудников и учащихся от "нежелательных материалов". Иногда блокировка происходит по IP-адресу названию сайта или по доменному имени. А иногда фильтруются поисковые запросы по незашифрованным соединениям со словами из "черного списка".

Фильтры практически всегда можно "обойти", используя компьютеры-посредники за пределами вашей страны. Они называются прокси и бывают самых разных типов.

Для того чтобы получить доступ к закрытым ресурсам необходимо сделать свой серфинг в интернете анонимным, когда не отслеживается ваше местоположение.

1. Первый инструмент который нам поможет это бесплатное расширение для браузера Хром FriGate

2. Браузер Tor. При выходе в интернет через Tor не отслеживается ваше местоположение, и никуда не записываются ваши данные: пароль, логины номера кредитных карт.

**Что такое прокси?**

Прокси-сервер (от англ. proxy - право пользоваться от чужого имени) - удаленный компьютер, который, при подключении к нему вашей машины, становится посредником для выхода абонента в интернет. Прокси передает все запросы программ абонента в сеть, и, получив ответ, отправляет его обратно абоненту.

**Что такое VPN?**

VPN (VirtualPrivateNetwork) – обобщенное название сети или соединения, которое создано внутри или поверх другой сети, например сети Интернет. Как правило, так называют созданную защищенную сеть или туннель внутри незащищенной сети Интернета. В самом простом виде VPN

представляет собой туннель из VPN клиента, установленного на компьютере пользователя и VPN сервера. Внутри этого туннеля, средствами VPN, осуществляется защита, шифрование и изменение данных, которыми обменивается компьютер пользователя и веб-сайты или веб-сервисы в сети Интернет.

**Как обезопасить себя и свои данные в социальных сетях?**

Социальные сети - не мода и не игрушка. Не стоит относиться к ним легкомысленно, сегодня это - мощный инструмент распространения информации, общения с аудиторией, поиска союзников и получения помощи. Их владельцы – коммерческие фирмы, а для них больше людей - значит, больше аккаунтов. Досье, если хотите.

Нам кажется, что социальная сеть – своего рода «продолжение Интернета», этакое свободное сообщество. Между тем, у каждой сети есть свой хозяин. Именно ему вы доверяете всю информацию. А он волен поступать с ней по-всякому. Например, круг

ваших знакомых. Сегодня вы своими руками добавляете аккаунты друзей и родственников в свой личный список. Завтра к владельцу социальной сети явятся правоохранительные органы и потребуют передать им этот список. Может ли такое случиться? Вполне.

Что касается начала работы, то первым делом следует вспомнить о надежном пароле. Самый короткий способ все разрушить (включая доверие коллег) - допустить, чтобы кто-нибудь посторонний получил доступ к вашему аккаунту. Будь это случайный человек или злоумышленник, он станет обладателем информации о вас и тех, с кем вы связаны. Поэтому пароль нужно правильно создавать, аккуратно хранить и регулярно менять.

**Как пользоваться сетью чтобы злоумышленники не использовали ваши данные?**

Для того, чтобы злоумышленники не использовали ваши данные, есть несколько простых решений. Вот несколько из них: - не надо без надобности размещать в

соцсетях информацию личного характера; не надо в соцсетях размещать много информации; не заводите большое количество аккаунтов в различных сетях, почтовых сервис службах; в случае необходимости заведения нескольких почтовых ящиков различайте их по тематикам (например, служебный, по подпискам к различным приложениям и т.д.), и при заполнении анкеты вносите минимум информации, используйте вымышленные имена, и автобиографию и тому подобнее.

**Как должны вести себя люди, и на какие сегменты (моменты) должны обратить внимание при распространении информации, чтобы она ни в коем случае не стала достоянием общественности или публичного доступа?**

Характерность социальных сетей такова, что в них можно завести множество друзей, найти знакомых, сослуживцев, людей с общими интересами и т.д. При этом не надо забывать, что близких друзей бывает немного, и не надо доверять им всем подряд, будьте выборочным и только с теми,

которых вы знаете очень хорошо, и очень долго, близки вам, будьте с ними самим собой.

**Все же если есть необходимость загружать и сохранить информацию в социальных сетях или интернете какие меры необходимо соблюдать?**

Не надо информацию опубликовывать, в случае размещения информации, надо смотреть на настройки (кому разрешено ознакомиться, кто имеет доступ и т.д.) т.е. внимательно изучите настройки рассылки.

**В чем заключается особенности разных сетей?**

Facebook - крупнейшая в мире социальная сеть. Если ваш новый знакомый или собеседник признается, что он активный пользователь интернета, с большой вероятностью у него есть аккаунт в Facebook. К сожалению, об этом известно и нашим недоброжелателям. Поэтому если кто-нибудь решил использовать интернет для составления досье или просто для сбора

информации о человеке, он, скорее всего, начнет с Facebook.

Стоит вам создать аккаунт в Facebook, вы не сможете его удалить. Facebook позволит лишь «деактивировать» аккаунт (по запросу), но в любой момент его можно восстановить со всей находящейся там информацией и настройками. Проще говоря, ваши данные из Facebook не удаляются.

«Условия использования» Facebook гласят, что для любых загруженных вами фотографий и видео вы передаете Facebook неисключительное право использовать эти материалы без географических ограничений. Facebook утрачивает это право, лишь когда вы удаляете свой аккаунт, или сами материалы. Однако если вы были настолько добры, что поделились материалами с кем-нибудь, и этот пользователь Facebook не удалил их, право сохраняется.

Twitter появился как служба обмена информацией типа «Что я сейчас делаю». Данные передавались с мобильных телефонов в интернет. Каждое сообщение укладывалось в 140 символов. Twitter называли «SMS для интернета». Система

позволяет другим пользователям следить за вашей жизнью, а вам, соответственно, интересоваться, как идут дела у других людей. В отличие от социальной сети, «интересующиеся» - вовсе необязательно друзья. Этот список мало даст тому, кто захочет установить ваш круг общения. С другой стороны, в Twitter проще манипулировать личностью, выдавать себя за другого человека.

YouTube - наиболее известная служба для публичного размещения и обмена видеоматериалами. Владелец этого сервиса - компания Google. YouTube очень удобно использовать, когда видеофайл нужно сделать доступным самой широкой аудитории. Однако, если сотрудники Google посчитают ваше видео противозаконным или даже спорным, его могут удалить. Таким образом, нельзя считать YouTube удачным местом для хранения видеоархива. Google известен своей готовностью к компромиссу в этом смысле: компания старается избежать претензий и блокировки сервиса.

Google фиксирует имена пользователей для всех загружаемых материалов, а также информацию, откуда поступил тот или иной ролик. Это может быть потенциально использовано для отслеживания пользователей.

Хотя вы сохраняете право собственности на материалы, выложенные в YouTube, компания Google автоматически получает разрешение распространять эти материалы.

Flickr - сервис для размещения, в первую очередь, фотоматериалов – принадлежит компании Yahoo!.

То, что вы размещаете на Flickr, остается вашей собственностью и может «облагаться» разными лицензиями и копирайтами. В свою очередь, вы даете Yahoo! разрешение распространять ваши материалы, выложенные на Flickr.

Flickr можно использовать не только для размещения фото, но и для поиска изображений с целью ис-пользования в работе. Многие лицензии, так или иначе позволяют это делать.

ВКонтакте - самая крупная российская социальная сеть, основанная в 2006 году с целью предоставить пользователям интернета возможность искать и находить одноклассников, сокурсников и т.д. Сегодня ВКонтакте является одним из самых популярных онлайновых сервисов не только в России, но и в ряде стран бывшего СССР. По своей идеологии ВКонтакте напоминает Facebook. Сеть бурно развивается, то и дело появляются новые функции, дополнения, изменения. Они нередко затрагивают и вопросы приватности. Так, в феврале 2011 года пользователи ВКонтакте лишились возможности ограничивать доступ к записям на своей страничке («стене»); с этих пор записи могут быть прочитаны кем угодно, включая тех, кто не зарегистрирован в социальной сети. Объявления такого рода могут происходить без предварительного уведомления пользователей.

Одноклассники – также известна как «Одноклассники.ру». Вторая по значимости социальная сеть в России, ближайший отечественный конкурент «ВКонтакте». «Одноклассники» созданы в том же 2006

году с той же целью. Вопросы, связанные с безопасностью и приватностью, «традиционны» для социальных сетей. В частности, если пользователь «Одноклассников» добавил друга или загрузил фотографию, всякий другой пользователь может отследить эти действия в «Ленте активности».

«Живой Журнал» (сокращенно ЖЖ) - не социальная сеть, а система ведения блогов, международная по статусу и крупнейшая в своем роде для России. ЖЖ несет в себе черты социальной сети (например, можно «зафрендить» другого пользователя). Пользователи ЖЖ, как правило, выступают под псевдонимами (никами), а не под настоящими именами. С другой стороны, будучи блоггерской системой, ЖЖ предназначен для регулярных публикаций и общения в т.н. сообществах. Из-за этого объем информации о частной жизни (взглядах, привычках, интересах) в ЖЖ очень велик.

**Выводы и советы:**

- Отыщите на веб-сайте социальной сети политику приватности (иногда

ее называют "политикой конфиденциальности") и прочтите то, что относится к безопасности ваших данных. Скажем, оставляет ли владелец сети за собой право использовать эту информацию в маркетинговых исследованиях?

- Выясните, какие программные способы предлагает владелец сети для защиты данных. Например, если вы заполните свой профиль, можно ли поставить нужную галочку, чтобы эта информация не показывалась другим пользователям?
- Если вы собираетесь провести какую-нибудь онлайновую акцию, возможно, следует завести для этого другой аккаунт, а не тот, который был использован в предыдущей акции. Или хотя бы другой псевдоним (ник).
- Так ли необходимо заполнять все поля вашего профиля, особенно если вы предполагаете использовать его в рабочих целях? Возможно, вы готовы поделиться фотографией, но вряд

ли нужно сообщать миру о деталях личной жизни, например, о детях, или о том, как вы привыкли проводить свободное время.

- Социальная сеть может содержать инструменты для интеграции с другими подобными сетями или сервисами. К примеру, вы публикуете что-нибудь в Twitter, и эта новость автоматически появляется на вашей страничке в Facebook. Будьте осторожны с интеграцией! На каком-либо ресурсе вы можете действовать анонимно и чувствовать себя защищенным, но лишь до поры и до времени. Интеграция-автоматика может раскрыть вашу личность.
- Никогда не используйте социальную сеть или иной подобный сервис в качестве основного хранилища информации. Это не ваш личный сайт, он вам не принадлежит, а резервное ко-пирование обычно не входит в набор стандартных инструментов. Если решением владельца (а может, и под давлением правительства) ваша

страница окажется заблокирована или удалена, жаловаться будет поздно. Помните, что владельцу сети проще избавиться от "неудобного" пользователя, чем вступать в конфликт с правительством, рискуя потерять гораздо больше.

- Привязывайте учетные записи к номеру телефона, используйте многоступенчатую идентификацию и аутентификации.

## IV. БЕЗОПАСНОСТЬ МОБИЛЬНОГО ТЕЛЕФОНА

Значительная часть нашей жизни сегодня зависит от мобильных телефонов. В них размещено столько данных, что защита личной информации становится насущной необходимостью. Современные мобильные телефоны оснащены новейшими системами обеспечения безо-пасности: среди них функции MobileTracker и ложный вызов, которые гарантируют максимальную сохранность Вашего телефона, Вашей личной информации и Вас самих.

Одной из проблем, связанных с тем, что мобильные телефоны занимают так много места в нашей жизни, является трудность восстановления информации в случае пропажи устройства - неважно, украдено оно или просто потеряно. Это не только трата времени, денег и нервов, но еще и вторжение в личное пространство. К счастью, есть выход.

**Как защитить себя и собственное устройство?**

Функция MobileTracker - одна из многих функций, которые способствуют возвра-

щению украденного или потерянного телефона к владельцу. Она работает так: когда в Ваш телефон или смартфон вставляют новую SIM-карту, устройство автоматически отправляет сообщение на заранее указанный номер. В сообщении указывается номер новой SIM-карты. Это поможет отследить новую SIM-карту и Ваше устройство - перспектива, которая отпугивает воров.

Другие важные меры обеспечения безопасности - это ложный вызов и приложение Listen-in. Оба включаются двойным нажатием кнопки. Функция ложного вызова (как можно догадаться по названию) заставляет Ваш телефон имитировать вызов. Это может быть очень удобно, если Вы находитесь в неприятной ситуации или хотите избежать разговора с кем-то. Иными словами, эта функция может оказаться полезной в самых разных случаях.

**Чем опасен мобильный телефон?**

Информационно-коммуникационные технологии не топчутся на месте. Сотовые телефоны "научились" определять GPS-

координаты, фотографировать, снимать видео и записывать разговоры. С их помощью можно читать книги, делать заметки и подключаться к Интернету. Рынок наполнился коммуникаторами и смартфонами. Почти каждый пользователь компьютера знаком с понятием "антивирус". Но далеко не каждый владелец сотового телефона представляет, чем он рискует, доверяя своему маленькому электронному помощнику деликатную информацию.

**Что мы знаем о безопасности мобильной связи?**

**1.** Такие сети контролируются или государством, или частными компаниями, которые следуют законным (но, бывает, и неофициальным) требованиям того же государства. Оператор имеет доступ к данным клиентов. При желании ему нетрудно перехватить звонок или текстовое сообщение. У оператора есть возможность отследить местонахождение устройства, а значит, и того, кто им в данный момент пользуется.

2. Производитель мобильного устройства - обычно и создатель, и настройщик программного обеспечения. Настройка осуществляется с учетом ожиданий разных провайдеров для использования в их сетях. Таким образом, операционная система может включать скрытые опции, которые делают возможным мониторинг со стороны провайдера или третьей стороны.

3. За последние годы в мобильных устройствах появилось множество новых функций. Пожалуй, такое устройство сегодня можно назвать портативным мини-компьютером с подключением к интернету, который, помимо прочего, играет роль мобильного телефона.

**Насколько опасно отправлять информации с мобильного телефона?**

Оператор мобильной связи имеет полный доступ ко всем текстовым и голосовым сообщениям, проходящим через его сеть. Во многих странах телефонные компании по закону обязаны хранить данные обо всех сеансах связи. В некоторых странах телефонная связь вообще является

государственной монополией. Наконец, голосовые и текстовые сообщения могут быть перехвачены третьей стороной с помощью сравнительно недорогого специального оборудования.

**Безопасно ли хранить информацию в мобильном телефоне?**

Сегодня мобильный телефон может хранить разные типы данных: историю звонков, текстовые сообщения (отправленные и полученные), адресную книгу, фотографии, видеоклипы, документы. По этой информации можно судить, например, о круге ваших интересов. Нетрудно представить, кто ваши ближайшие друзья, чем они занимаются, и так далее. Защитить такую информацию непросто, а в некоторых телефонах невозможно.

Больше функций - выше риск. А если мобильник подключается к интернету, возникает целый спектр проблем, которые уже известны пользователям компьютеров и компьютерных сетей.

**Какие данные уязвимы, если речь идет о мобильной связи?**

Вот некоторые примеры.

- История звонков (номер, время, продолжительность разговора).
- SMS-сообщения.
- Адресная книга.
- Календарь с планируемыми встречами.
- Текстовые заметки.
- Фотографии и видеозаписи.

Очень многие люди доверяют сотовому телефону массу важной информации. Потеря "мобильника" приводит человека в отчаяние. Но что если телефон украден? А доступ к нему ничем не защищен? Даже короткий PIN-код вводить не нужно (так сейчас настроены многие сотовые телефоны)?

Компании сотовой связи регистрируют всякую передачу и прием данных по номеру вашего телефона, идентификационный номер устройства и номер SIM-карты. В большинстве государств установлен порядок приобретения SIM-карты только при предъявлении документов удо-

стоверяющей личности, в связи с чем заинтересованной стороне нетрудно установить личности владельцев телефона.

**Как защитить данные на мобильном телефоне?**

Как и с компьютерами, на первом месте — физическая защита.

- Держите сотовый телефон при себе. Не оставляйте его вне поля зрения и не давайте другим людям "попользоваться".
- Включите стандартную защиту - запрос PIN-кода. Держите PIN-код в памяти, не записывайте на бумажку, вложенную в кошелек или паспорт. Используйте свой пин-код, а не значение по умолчанию.
- Пометьте каким-нибудь способом SIM-карту, карточку памяти, аккумулятор и корпус самого телефона. Эти метки должны быть малозаметными, не привлекать внимание. Их значение – засвидетельствовать, что среди компонентов телефона не было подмены. Если вы продвинутый пользователь, неплохая идея - попробовать ультрафиолетовые маркеры, которые не видны при обычном свете. Можно также

исполь-зовать специальные защитные микронак-лейки на защелки и шурупы, которыми скреплены детали корпуса. Это придаст вам уверенность, что телефон никем не разбирался.

- Следует четко знать, какие данные записаны на мобильном устройстве. Не стоит хранить в сотовом телефоне деликатную информацию. Если все-таки нечто подобное приходится держать на телефоне, подумайте: может быть, лучше записывать на дополнительную карточку памяти, которую в случае опасности легко вытащить из телефона и уничтожить.
- Если приходится ремонтировать телефон, или вы решили его подарить/продать, не забудьте вынуть сим-карту и карту памяти, а также очистить адресную книгу, список SMS и прочие разделы.
- Когда устанавливаете новую сим-карту, позаботьтесь о том, чтобы никакие данные не "застряли" на предыдущей. А если замена временная, нужно следить, чтобы вынутая сим-карта нигде не валялась и не попадала в руки, кому не нужно.

• По возможности выбирайте только тех операторов связи и магазины/продавцов, которые пользуются (более-менее) солидной репутацией. Для серьезной работы, особенно связанной с общественной деятельностью в условиях повышенного внимания государства к вашей организации, вряд ли стоит покупать мобильный телефон "с рук" у незнакомого человека. Если вы склонны часто менять телефоны, не приобретайте их все время в одном и том же месте. Это снизит риск, что следующий аппарат будет снабжен особой программной "начинкой" специально для вас.

• Не забывайте делать резервные копии всех данных, копируйте их на компьютер. Позаботьтесь о том, чтобы данные хранились в безопасном месте. В экстренном случае вы сможете восстановить важную информацию. Кроме того, если телефон был изъят, потерян или украден, вы будете наверняка знать, какие данные скомпрометированы.

• Каждый аппарат имеет 15-значный уникальный код (IMEI). Он однозначно идентифицирует телефон. В большинстве

моделей узнать IMEI можно, набрав *#06#. Код может быть написан на корпусе под аккумулятором. Запишите этот код и храните отдельно от телефона. Знание кода может послужить доказательством того, что аппарат действительно принадлежит вам.

- Иногда можно зарегистрировать телефон у оператора связи. В случае пропажи аппарата его использование нетрудно блокировать. Следует помнить, однако, что в таком случае данный телефон будет прочно (и документировано) связан с вашей личностью.

**Как осуществляется слежка с использованием вашего мобильного телефона?**

Всякий сотовый телефон регулярно и автоматически "выдает" провайдеру информацию о своем местоположении. Многие телефоны снабжены функциями GPS. Данные о местоположении можно добавлять к другой информации, например, фотоснимкам и SMS.

Когда мы делаем звонок по мобильному телефону, аппарат устанавливает связь

с ближайшими сотовыми вышками. Таким образом, оператор сотовой связи, в принципе, знает точное местонахождение телефона.

Как правило, злоумышленника интересует не аппарат, а его владелец. Чтобы осуществлять эффективную слежку за человеком, нужно быть уверенным, по крайней мере, что этот телефон принадлежит именно ему.

Пока телефон включен, он поддерживает контакт с вышками сотовой связи, даже если ты не разговариваешь, даже в выключенном состоянии телефон может быть активным, так как мобильный телефон - электронное устройство, передатчик. Пока есть источник питания, сохраняется вероятность (пусть и очень маленькая), что кто-нибудь сумеет включить телефон без вашего ведома. Поэтому проще всего при отсутствии надобности не брат с собой телефон. В случае выключения лучше вытащить аккумулятор.

**Как сохранить анонимность при использовании телефонных звон-ков?**

Если вам приходится обмениваться по телефону деликатной информацией, советуем пользоваться нижеследующими рекомендациями:

- Звоните из разных мест. Лучше, если эти места нельзя будет однозначно связать с вашей личностью.
- Если вы серьезно опасаетесь за свою жизнь и уверены, что за вами могут следить, то приобретайте привычку в случае отсутствия необходимости пользоваться телефоном постоянно вынимать аккумулятор. Такое поведение сильно затруднит жизнь тому, кто вознамерится вас отследить.
- Меняйте телефонные аппараты. Меняйте сим-карты.
- Если позволяют законы страны, покупайте сим-карту без регистрации, предоставления документов и заполнения анкет.
- Не платите за мобильную связь кредитной карточкой. Такие карточки всегда именные.

**Как защитить телефон от прослушки?**

Любой мобильный телефон можно прослушать. Прослушку телефона можно включить даже на телефоне, находящемся в режиме ожидания (то есть с «положенной трубкой»). При этом без защиты от прослушки никаких видимых признаков на экране смартфона или изменений качества связи Вы не обнаружите. Факт прослушки в цифровых мобильных сетях определить попросту невозможно. Для того, чтобы снизить вероятность прослушки мобильного телефона до минимума, необходима защита сотовых телефонов (защита мобильных телефонов). Модуль защиты мобильного телефона от прослушки встроен в комплексный пакет защитного программного обеспечения SpyDetector.

**По каким признакам можно догадаться о наличии прослушки в телефоне?**

Признаки: батарея быстро истощается, самопроизвольно загружается, включается подсветка, соединении с абонементом про-

исходит очень долго, слышны посторонние голоса и звуки, при поднесении к аудиоколонкам телефон будет создавать помехи в то время когда к вам никто не звонит.

**Есть ли возможность выявить прослушки вашего телефона?**

В интернете приводятся множество способов выявления самим прослушки, но никакой из них не может быть гарантийным. В отличие от аналоговых телефонных линий, где установить вмешательство прослушки достаточно легко, определить прослушивание мобильных телефонов, то есть установить факт прослушки сотового без специальной аппаратуры невозможно, так как сотовые сети, обеспечивающие разговоры по мобильным телефонам работают по иным техническим принципам и исключают подобную возможность. А выявить с помощью специальных технических средств т.е. обратиться к специалистам дорогое удовольствие. Единственное что вы можете себе позволить это

установить на своем телефоне программы антиспай.

**Как снизить вероятность прослушивания мобильного телефона, обеспечить защиту от прослушки?**

- Сведите к минимуму, а лучше исключите вовсе передачу конфиденциальной информации по мобильному телефону, в первую очередь такой, как номера кредитных карточек, финансовые вопросы, пароли.
- Не применяйте сотовые (мобильные) телефоны для ведения важных деловых разговоров. При необходимости пользуйтесь специально подготовленными мобильными телефонами или системами пространственного зашумления.
- Важно: телефонный разговор, который ведется с движущегося автомобиля гораздо труднее перехватить, поскольку расстояние между ним и перехватывающей аппаратурой (если та находится не в автомобиле) увеличивается и сигнал ослабевает.

• Используйте системы мобильной связи, в которых данные передаются при частой автоматической смене частот в течение разговора (к примеру, GPRS).

• Полностью отключите свой мобильный телефон (снимите батарею), если хотите сохранить в тайне ваше местонахождение. Почувствовав слежку, иногда полезно оставить включенный телефон в машине или кабинете, проследовав на важную встречу без него.

• Никогда не ремонтируйте телефон в непроверенных мастерских.

**Есть ли вероятность перехвата ваших телефонных звонков?**

Как правило, и голосовые, и текстовые мобильные коммуникации не могут похвастать высоким уровнем защиты (шифрования). Есть сравнительно недорогие технологии, с помощью которых нетрудно перехватить отправляемый текст или подслушать разговор. Все, что нужно злоумышленнику - доступ к телефону. Кроме того, оператор связи в курсе ваших переговоров. Сегодня еще не построена

такая система общедоступной мобильной связи, которая, с одной стороны, эффективно шифровала бы данные (например, с помощью алгоритмов стойкой криптографии), а с другой стороны, соответствовала бы законам государств и интересам их спецслужб. Сегодня для использования криптографии нужно установить в телефоне соответствующую программу, а потом сделать то же самое для аппарата собеседника. Подобное пока возможно только в нескольких моделях смартфонов.

**Насколько безопасна общение посредством текстовых сообщений (SMS)?**

Если нужно отправить информацию так, чтобы она гарантированно не попала в чужие руки, вряд ли стоит полагаться на SMS. Этот способ текстовых ком-муникаций не обеспечивает конфи-денциальность. Обладая желанием и техническими возможностями, перехватить SMS так же просто, как голосовое сообщение. Третье лицо получит доступ к тексту сообщения и

телефонным номерам отправителя и адресата. Кроме того, SMS можно изменить или подделать.

Во многих странах существует законодательное (а кое-где и не вполне законное) требование к операторам связи хранить все текстовые сообщения, отправленные/принятые их клиентами. Срок хранения может растянуться на годы. Как правило, это требование обосновывается необходимостью борьбы с преступностью, в частности, терроризмом. Порой и сами операторы связи совершают подобные действия для маркетинговых и статистических задач.

Очень часто SMS-сообщения образуют в памяти телефона целый архив. Если кто-нибудь украдет ваш телефон или просто получит к нему доступ, он сможет прочесть эти сообщения. Выработайте привычку удалять "смски" сразу после прочтения.

В некоторых моделях телефонов можно отключить запись информации о телефонных звонках и SMS.

**К каким дополнительным мерам безопасности еще можно прибегнут при использовании мобильного телефона?**

Мобильные телефоны приобретают черты, которые все больше роднят их с компьютерами. Сегодня многие пользуются коммуникаторами и смартфонами, где установлены операционные системы и запускаются приложения. Можно скачать из сети программу, установить ее и работать — всё как на обычном компьютере. Это может повлечь распространения вирусов и прочего вредоносного кода.

- Не храните конфиденциальную информацию в телефоне. Фотографии, видеозаписи, SMS. Как только предоставляется возможность, перемещайте их на компьютер, в безопасное хранилище.
- Почаще стирайте записи о телефонных звонках, сообщениях, ненужные (необязательные) контакты в адресной книге, и так далее.
- Если вы хотя бы иногда выходите в интернет с мобильного телефона, по возможности пользуйтесь для передачи данных "защищенным" протоколом SSL.

• Подключайте телефон к компьютеру только тогда, когда твердо уверены, что оба устройства свободны от вирусов и другого вредоносного кода.

• Не скачивайте и не устанавливайте в телефон незнакомые и непроверенные программы, рингтоны (мелодии звонков), обои (графическое оформление), Java-приложения и вообще что бы то ни было из источников, чья надежность не подтверждена.

• Обращайте внимание на то, как работает ваш сотовый телефон. Новая незнакомая программа, какой-то непривычный процесс, странное сообщение, нестабильная работа — все это поводы задуматься. Если какие-то программы вам не нужны, проще (и лучше) всего отключить их или вообще удалить из телефона (если это позволяют средства операционной системы).

• Будьте аккуратны, используя открытые точки Wi-Fi.

• Убедитесь, что беспроводная связь (инфракрасная, Bluetooth, WiFi, WiMax и другие) на вашем телефоне отключены, если

только вы не пользуетесь ими в данный момент. Модули беспроводной связи лучше включать с осторожностью и в надежных, проверенных местах. По возможности лучше вообще избегать пользоваться Bluetooth, так как эта технология сравнительно легко под-вергается контролю со стороны третьих лиц (проще говоря, "прослушиванию"). Лучше использовать для связи кабель, а если речь о наушниках или гарнитурах, то не беспроводные (Bluetooth), а менее удобные, но лучшие с точки зрения безопасности проводные.

**Выводы и советы:**

Чтобы сохранить конфиденциальность и безопасность при использовании телефонов, как и в случаях с компьютерами и другими техническими средствами обмена информации, следуйте так:

- Увеличьте безопасность своего мобильного телефона, используя советы SaferMobile и Security-in-a-Box.
- Всегда держите телефон при себе, защищенный паролем, который не так легко

угадать остальным. Никогда не говорите этот пароль другим.

- Если вы переживаете о сохранении анонимности, часто меняйте телефоны и SIM карты (стирая предварительно все данные). Только изменение SIM карты недостаточно для защиты вашей конфиденциальности.
- Используйте незарегистрированные SIM карты с предоплатой, если это возможно. Всегда платите за карты наличными.
- Если вы обеспокоены тем, что ваши движения могут быть отслежены, носите телефон выключенным, с вытащенной батареей, пока вы придете в безопасное место, где вы можете звонить. После вызова, выключите телефон и снимите батарею. Если вы делаете это после каждого вызова, телефон не может быть использован для отслеживания движений.

## V. ЗАКОНОДАТЕЛЬНАЯ БАЗА ПО ЦИФРОВОЙ БЕЗОПАСНОСТИ

### *Извлечения из Уголовного Кодекса РТ*

**Статья 144. Незаконное собирание и распространение информации о частной жизни**

1) Незаконное собирание или распространения сведений о частной жизни, составляющих личную или семейную тайну другого лица, без его согласия либо распространение таких сведений в публичном выступлении, произведении, средствах массовой информации или сети интернет если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам гражданина,

- наказывается обязательными работами на срок от ста двадцати до ста восьмидесяти часов или штрафом в размере от двухсот до пятисот показателей для расчётов либо исправительными работами до одного года либо арестом на срок до четырех месяцев.

2) Те же деяния, совершенные лицом с использованием своего служебного положения,

- наказываются штрафом в размере от пятисот до восьмисот показателей для расчётов либо исправительными работами до двух лет либо арестом на срок до шести месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

**Статья 146. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений**

1) Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан,

- наказывается обязательными работами на срок от ста до ста шестидесяти часов или штрафом в размере до двухсот показателей для расчётов либо исправительными работами до одного года.

2) Те же деяния, совершенные лицом с использованием своего служебного положения или специальных технических

средств, предназначенных для негласного получения информации,

- наказываются штрафом в размере от двухсот до пятисот показателей для расчётов либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет либо арестом на срок от двух до четырех месяцев.

3) Незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации,

- наказывается штрафом в размере от пятисот до восьмисот показателей для расчётов или лишением права занимать определенные должности или заниматься определенной деятельностью на срок от пяти до десяти лет или ограничением свободы на срок до пяти лет.

**Статья 147. Нарушение неприкосновенности жилища**

1) Незаконное проникновение в жилище, совершенное против воли прожи-

вающего в нем лица, либо лишение кого-либо жилища,

- наказывается штрафом в размере от одной до двух тысяч показателей для расчётов либо лишением свободы до двух лет.

2) Те же действия, совершенные:

а) с применением насилия или угрозы его применения;

б) с использованием служебного положения;

в) с незаконной установкой в жилом помещении подслушивающих или иных специальных устройств,

- наказываются лишением свободы на срок от двух до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

**Примечание:**

Под жилищем в настоящей статье, а также в других статьях настоящего Кодекса понимаются индивидуальный жилой дом с входящими в него жилыми и нежилыми помещениями, жилое помещение, незави-

симо от формы собственности, входящее в жилищный фонд и пригодное для постоянного или временного проживания, а равно иное помещение или строение, не входящее в жилищный фонд, но предназначенное для временного проживания.

**Статья 148. Отказ в предоставлении гражданину информации**

Незаконный отказ должностного лица в предоставлении гражданину документов или материалов, непосредственно затрагивающих его права и свободы и собранных в установленном порядке, а равно предоставление лицу неполной или умышленно искаженной такой информации, если это причинило ущерб правам и интересам данного гражданина,

- наказывается штрафом в размере от трехсот до пятисот показателей для расчётов либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от трех до пяти лет.

**Статья 149. Незаконное ограничение передвижения, свободного выбора места жительства, выезда за пределы республики и возвращения гражданина**

1) Незаконное ограничение прав передвижения, свободного выбора места жительства, выезда за пределы республики и возвращения гражданина,

- наказываются штрафом в размере от одной до двух тысяч показателей для расчётов либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2) Те же деяния, если:

а) стали причиной тяжких последствий;

б) совершены лицом с использованием своего служебного положения,

- наказывается лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок от трех до пяти лет.

**Статья 158. Воспрепятствование деятельности политических партий и общественных объединений**

Воспрепятствование законной деятельности политических партий, общественных объединений, а равно вмешательство в законную их деятельность, повлекшее существенное нарушение их прав и законных интересов,

- наказывается штрафом в размере от двухсот до пятисот показателей для расчётов либо ограничением свободы сроком до трех лет либо арестом на срок до четырех месяцев.

**Статья 162. Воспрепятствование законной профессиональной деятельности журналиста**

1) Воспрепятствование в какой бы то ни было форме законной профессиональной деятельности журналиста, а равно принуждение его к распространению либо отказу от распространения информации, соеди-ненное с угрозой насилия, уничтожением или повреждением имущества, распространением клеветнических измышлений или

оглашением иных сведений, которые потерпевший желает сохранить в тайне, а равно путем угрозы ущемления прав и законных интересов журналиста,

- наказывается штрафом в размере от пятисот до восьмисот показателей для расчётов либо исправительными работами на срок до двух лет, либо арестом на срок до шести месяцев.

2) Те же деяния, сопряженные:

а) насилием;

б) уничтожением или повреж-дением имущества;

в) с использованием своего служебного положения,

- наказывается ограничением свободы сроком до трех лет или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо без такового.

**Статья 163. Нарушение законнодательства об обращении граждан**

1) Неправомерный отказ в рассмотрении обращения граждан, нарушения

без уважительных причин сроков рассмотрения обращений, принятие необоснованного, противоречащего закону решения, а также нарушения законодательства об обращении граждан, причинившие существенный вред правам либо охраняемым законом интересам граждан, общества или государства,

- наказываются штрафом в размере от пятисот до восьмисот показателей для расчётов либо исправительными работами до двух лет, либо арестом на срок до шести месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2) Преследование гражданина должностным лицом в связи с его обращением в государственный орган, на предприятие в учреждение, организацию, общественное объединение либо за содержащуюся в обращении критику, а равно за выступление с критикой в иной форме, - наказывается штрафом в размере от тысячи пятисот до двух тысяч показателей для расчётов либо ограничением свободы на срок на срок до

пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок от трех до пяти лет.

**Статья 298. Неправомерный доступ к компьютерной информации**

1) Неправомерный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты,

- наказывается штрафом в размере от двухсот до четырехсот показателей для расчётов либо лишением свободы на срок до двух лет.

2) Те же деяния, повлекшие по неосторожности изменение, уничтожение либо блокирование информации, а равно вывод из строя компьютерного оборудования, либо значительный ущерб,

- наказываются штрафом в размере от трехсот до пятисот показателей для расчётов либо исправительными работами на срок до двух лет либо лишением свободы на срок до трех лет.

3) Деяния, предусмотренные частью первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия,

- наказываются штрафом в размере от четырехсот до семисот показателей для расчётов либо лишением свободы на срок до четырех лет.

**Статья 299. Модификация компьютерной информации**

1) Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, а равно внесение в них заведомо ложной информации, причинившее значительный ущерб или создавшее угрозу его причинения,

- наказывается штрафом в размере от трехсот до пятисот показателей для расчётов, либо исправительными работами на срок до двух лет либо лишением свободы на тот же срок.

2) То же деяние:

а) сопряженное с неправомерным доступом к компьютерной системе или сети;

б) повлекшее по неосторожности тяжкие последствия,

- наказывается штрафом в размере от пятисот до одной тысячи показателей для расчётов либо лишением свободы до трех лет .

**Статья 300. Компьютерный саботаж**

1) Уничтожение, блокирование либо приведение в непригодное состояние компьютерной информации или программы, вывод из строя компьютерного оборудования, а равно разрушение компьютерной системы, сети или машинного носителя,

- наказывается штрафом в размере от двухсот до пятисот показателей для расчётов или ограничением свободы на срок до двух лет либо арестом на срок до четырех месяцев.

2) То же деяние:

а) сопряженное с неправомерным доступом к компьютерной системе или сети;

б) повлекшее по неосторожности тяжкие последствия,

- наказывается штрафом в размере от пятисот до одной тысячи показателей для

расчётов либо лишением свободы до трех лет.

**Статья 301. Незаконное завладение компьютерной информацией**

1) Незаконное копирование или иное неправомерное завладение инфор-мацией, хранящейся в компьютерной системе, сети или на машинных носителях, а равно перехват информации, передаваемой с использованием компьютерной связи,

- наказывается штрафом в размере от двухсот до пятисот показателей для расчётов либо лишением свободы до двух лет.

2) Принуждение к передаче инфор-мации, хранящейся в компьютерной системе, сети или на машинных носителях, под угрозой оглашения позорящих сведений о лице или его близких, предания гласности сведений о таких обстоятельствах, которые потерпевший желает сохранить в тайне, а равно под угрозой применения насилия над лицом или его близкими либо под угрозой уничтожения или повреждения имущества лица, его близких и других лиц, в ведении

или под охраной которых находится эта информация,

- наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок от двух до четырех лет.

3) Деяния, предусмотренные частями первой или второй настоящей статьи:

а) сопряженные с применением насилия над лицом или его близкими;

б) совершенные по предва-рительному сговору группой лиц;

в) причинившие значительный ущерб потерпевшему;

г) совершенные с целью получения особо ценной информации,

- наказываются лишением свободы на срок от пяти до семи лет.

4) Деяния, предусмотренные частями первой, второй или третьей настоящей статьи:

а) совершенные повторно;

б) совершенные организованной группой;

в) повлекшее по неосторожности смерть человека либо иных тяжких послед-ствий,

- наказывается лишением свободы на срок от семи до десяти лет.

**Статья 302. Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети**

Изготовление с целью сбыта, а равно сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети,

- наказывается штрафом в размере от двухсот до пятисот показателей для расчётов или ограничением свободы на срок до двух лет или арестом на срок от двух до шести месяцев.

**Статья 303. Разработка, использование и распространение вредоносных программ**

1) Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информа-

ции, хранящейся в компьютерной системе, сети или на машинных носителях, а также разработка специальных вирусных программ, заведомое их использование или распространение носителей с такими программами,

- наказывается штрафом в размере от трехсот до пятисот показателей для расчётов либо ограничением свободы на срок до двух лет.

2) То же деяние, повлекшее по неосторожности тяжкие последствия,

- наказывается штрафом в размере от пятисот до одной тысячи показателей для расчётов либо лишением свободы до трех лет.

**Статья 304. Нарушение правил эксплуатации компьютерной системы или сети**

1) Нарушение правил эксплуатации компьютерной системы, или сети лицом, имеющим доступ к этой системе или сети, если это повлекло по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение

работы компьютерного оборудования или причинение иного значительного ущерба,

- наказывается штрафом в размере до трехсот показателей для расчётов, либо ограничением свободы на срок до двух лет.

2) То же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности,

- наказывается штрафом в размере от трехсот до пятисот показателей для расчётов либо исправительными работами на срок до двух лет или лишением свободы на тот же срок.

3) Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия,

- наказываются штрафом в размере от пятисот до одной тысячи показателей для расчётов либо лишением свободы до трех лет.

# СПИСОК ИСПОЛЗОВАННОЙ И РЕКОМЕНДУЕМОЙ ДЛЯ ЧТЕНИЯ ЛИТЕРАТУРЫ


1. Security in-a-box(tools and tactics for your digital security), https://**securityinabox.org/**
2. Руководства по безопасности журналистов, КЗЖ, www.cpj.org
3. "Управление уровнем конфиденциальности" - материал, подго-товленный администрацией Facebook.
4. A Brief Introduction to Secure SMS Messaging in MIDP - Nokia developer guide ("Краткое введение в тему безопасного использования SMS-сообщений") *(англ.)*
5. A Guide to Mobile Phones – A short guide, for activists, to using mobile phones safely and securely ("Безопасность мобильных телефонов — Краткое руководство для активистов по безопасному использованию мобильных телефонов") *(англ.)*
6. A Guide to Mobile Security for Citizen Journalists ("Руководство по мобильной безопасности для гражданских журналистов"), подготовленное MobileActive.org *(англ.)*
7. CCleaner FAQ ("Вопросов и ответов" о CCleaner) *(англ.)*.
8. On LocationalPrivacy, and How to Avoid Losing it Forever ("Где вы находитесь: как не потерять приватность навсегда") - специиальное пособие

американской правозащитной организации Electronic Frontier Foundation.
9. Phones used as spying devices ("Телефоны как шпионские устройства") *(англ.)*
10. Security for Activists - A Practical Security Handbook for Activists and Campaigns ("Безопасность для активистов - практическое руководство для активистов и кампаний") *(англ.)*
11. The Mobile Advocacy Toolkit ("Инструменты для мобильного активиста").
12. TrueCrypt FAQ ("Вопросы и ответы о TrueCrypt") содержат базовую и весьма полезную информацию о TrueCrypt*(англ.)*.
13. Бесплатные онлайн-сервисы для удобного хранения небольшого объема важных данных, предварительно зашифрованных, в частности, Dropbox и ADrive*(англ.)*.
14. Википедия *(англ.)*.
15. Монография Петера Гуттмана о надежном удалении данных.
16. Руководства Digital Security and Privacy for Human Rights Defenders ("Цифровая безопасность и приватность для правозащитников") *(англ.)*.

## СОДЕРЖАНИЕ



Распространяется бесплатно.
Тираж 200 экз.