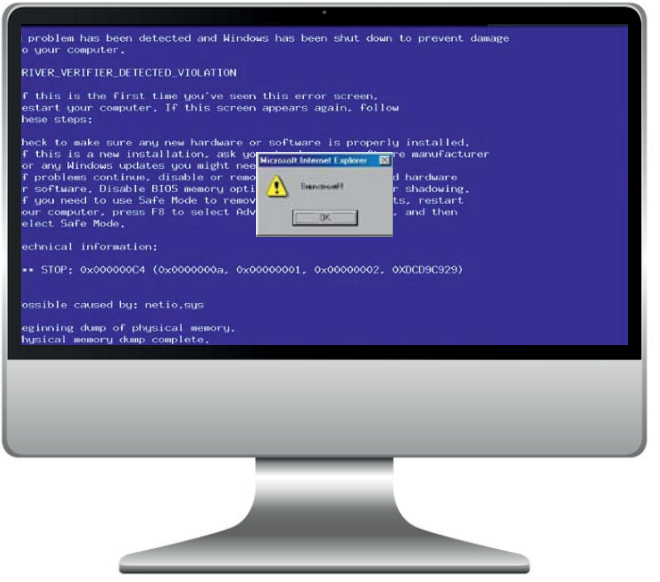
САНКТ-ПЕТЕРБУРГ ДЕТСКИЙ ХОСПИС



Пащенко Г. В.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ОКАЗАНИИ СОЦИАЛЬНЫХ УСЛУГ

Рекомендации для НКО по защите информации

Санкт-Петербург
2021

Пащенко Григорий Валентинович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ОКАЗАНИИ СОЦИАЛЬНЫХ УСЛУГ

Рекомендации для НКО по защите информации

Санкт-Петербург
2021

УДК 681.3
ББК 32.97 (А68)

Автор:
Пащенко Г. В. – руководитель проекта «КиберМосква»

Информационная безопасность при оказании социальных услуг
Рекомендации для НКО по защите информации

ISBN 978-5-906804-09-9

СОДЕРЖАНИЕ:

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОНТЕКСТЕ РАЗВИТИЯ НЕКОММЕРЧЕСКОГО СЕКТОРА

На современном этапе развития социума информация представляет собой определенную ценность. Не зря современное общество характеризуется как информационное, тогда как предыдущую фазу его развития назвали индустриальной.

Вопросы информационной безопасности стали особенно актуальны для России начиная с 90-х гг. XX века. Первый документ, устанавливающий основные термины и определения в области защиты информации в России, был издан в 1992 году Гостехкомиссией РФ под названием «Термины и определения в области защиты от НСД к информации. Руководящий документ Гостехкомиссии России».

«Выросшая» из вопросов технологий обработки и передачи информации в коммерческой сфере, теория информационной безопасности постоянно развивается и расширяет свое влияние на некоммерческие организации и государственный сектор.

Современные технологии преобразуют целые сектора экономики, включая общественные, благотворительные и некоммерческие организации.

При этом возможности, которые открывает цифровая трансформация общества для некоммерческих организаций, также формируют новые задачи по обеспечению информационной безопасности. Общественным организациям и государственным учреждениям, работающим с особенно чувствительной для общества проблематикой, – темами детства, помощи тяжелобольным гражданам, социализации детей-сирот и пр. – необходимо пересмотреть систему работы и адаптировать к новым реалиям и технологическим услови-

ям целый ряд задач. Речь идет о документационном сопровождении деятельности, организационных основах работы, подготовке волонтеров и сопровождении волонтерских программ, коммуникационных аспектах деятельности. Все эти составляющие нуждаются в критической оценке в контексте обеспечения информационной безопасности.

С точки зрения теории информационной безопасности ее предметной областью являются:

- информация и ее свойства;
- угрозы безопасности информации и ее собственникам;
- политика безопасности и модели безопасности;
- способы, методы и средства защиты информации;
- классификация систем защиты;
- требования к защищенности информационных систем;
- методология оценки защищенности информационных систем и проектирования защиты.
- конкретные системы защиты информации, применяемые в различных органах управления, учреждениях и на предприятиях различных форм собственности.

Так как предметной областью информационной безопасности является информация и все что с ней связано, основные понятия, термины и определения в области защиты информации одинаковы для любой организации вне зависимости от ее организационно-правовой формы.

Основные термины и определения по данной тематике приводятся в конце книги в разделе «Глоссарий».

2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ НЕКОММЕРЧЕСКИХ ОРГАНИЗАЦИЙ

Почему вообще возникла тема интернет- и информационной безопасности в сфере НКО? Казалось бы, современные некоммерческие организации не являются распорядителями больших бюджетов, суперсекретных технологий или носителями мегаважных тайн…

Да, общественные, некоммерческие и благотворительные организации просто делают свое дело, помогая людям, развивая волонтерские программы, организуя помощь особо уязвимым группам. Но дело в том, что ситуация в этой сфере довольно быстро меняется. В третьем секторе появились сильные организации, финансово хорошо обеспеченные, имеющие большое количество волонтеров и сотрудников. За последние 10–15 лет резко шагнули вперед технологии сбора средств с использованием банковских карт, запущены мощные программы фандрайзинга, а значит, НКО стали работать с информацией о благотворителях и их персональными данными. Следовательно, эти организации стали привлекательными для мошенников.

Более того, организации третьего сектора стали обладателями ценной информации, в которой заинтересованы мошенники, но при этом большинство НКО не успело перестроиться под эту новую реальность и по-прежнему достаточно беспечно относится к проблеме безопасности данных.

Обычно на семинарах мы предлагаем участникам очень простой тест, наглядно демонстрирующий, насколько уязвимы наши некоммерческие организации и какие риски обычно «не замечают» сотрудники НКО.

Итак, если Вы или Ваши сотрудники:

- храните информацию о своих благополучателях на компьютерах…
- создаете свои базы данных и храните на компьютере адреса, телефоны, даты рождения и другие данные волонтеров, клиентов, журналистов …
- ведете закрытую для посторонних группу в соцсетях (в которой, например, волонтеры обмениваются информацией друг с другом)…
- ведете онлайн-консультирование (например, предлагаете анонимные консультации психолога для подростков)…
- пользуетесь флешками, дисками для копирования и передачи информации…
- обсуждаете Ваших благотворителей, благополучателей в закрытых чатах, группах в популярных мессенджерах…

Если Вы отметили хотя бы один из пунктов этого теста, это значит, что Ваша организация находится в зоне риска и может столкнуться с реальными киберугрозами. Эти ситуации ведут не только к потере информации или краже денег. Это Ваши репутационные риски. Возможно, Вам пора задуматься над следующими вопросами:

Как оценить существующий уровень информационной безопасности в организации? Какие участки Вашей работы являются «слабыми звеньями» с точки зрения информационной безопасности? Насколько активно НКО использует средства защиты? Как предотвратить несанкционированное воздействие на информационную среду и как предупредить случайную утечку информации?

В данном пособии мы постараемся помочь Вам найти ответы на эти вопросы.

3. СПЕЦИФИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ПАЛЛИАТИВНОЙ ПОМОЩИ ДЕТЯМ: РИСКИ И ВОЗМОЖНОСТИ

В настоящее время вопросы информационной безопасности переходят в разряд острых проблем, актуальных не только для специалистов помогающих профессий, оказывающих помощь социально уязвимым группам. Особенно актуальной данная проблематика становится для детей и подростков, проводящих значительную часть времени в интернет-пространстве. В силу заболевания для многих пациентов паллиативных служб интернет становится окном в мир, возможностью общаться, дружить и развиваться.

В связи с тем, что школьная программа обучения не дает достаточных знаний и тем более навыков безопасного поведения в сети, молодые люди не умеют определять мошенничество, не знают, как поступать при столкновении с негативным или запрещенным контентом, с проявлениями буллинга, хейтерства.

С другой стороны, представители госучреждений и НКО зачастую не располагают достаточными ресурсами для обеспечения безопасности при хранении персональных данных своих благополучателей, а также не имеют возможности для регулярного повышения уровня знаний своих сотрудников в сфере интернет-безопасности.

Актуальность данной темы также подтверждает широкий общественный резонанс, который получают новости, связанные с проблемой интернет-безопасности, а также возросшее число обращений по данной теме в правоохранительные структуры и к Уполномоченному по правам ребенка.

Остановимся подробнее на особенностях информационной безопасности в сфере паллиативной помощи детям. Эти факторы были выявлены во время аудита информационной

безопасности, проведенного в 2020 году в паллиативных службах трех российских регионов, и мы рекомендуем их учитывать при разработке требований безопасности в сфере паллиативной помощи:

1. Непрерывность оказания паллиативной помощи детям. Если в других областях можно позволить себе взять время на решение возникающих проблем – банковские операции можно приостановить, продажи можно прервать, поставки задержать, – то в сфере паллиативной помощи речь идет о жизни детей. Все услуги должны оказываться непрерывно.

2. Активное включение волонтеров. Этот фактор может работать на позитивный результат (информационное волонтерство, например, способно решать множество задач в сфере паллиативной помощи), но может и представлять собой источник серьезного риска, если волонтеры допускаются к работе с информацией без достаточной подготовки и организационного сопровождения.

3. Большой объем персональной информации, в том числе медицинские сведения, информация о состоянии семьи и пр.
   Очевидно, что работа паллиативной медицинской службы сопряжена с хранением, анализом и обработкой конфиденциальной информации, распространение которой может нанести серьезный вред как близким пациента, так и самой организации, призванной оказывать помощь семье, столкнувшейся с тяжелым испытанием – болезнью ребенка.

4. Подключение к интернету большого количества неконтролируемых сторонних гаджетов (смартфонов, планшетов и прочих устройств сотрудников, пациентов, родственников пациентов) создает угрозу использования этой техники для взлома системы.

5. Недостаточное внимание к вопросам информационной безопасности, характерное для многих социально ориентированных организаций и лиц помогающих профессий.

Многие сотрудники социальных учреждений недооценивают важность информации, с которой они работают. Большая часть выявленных существующих и потенциальных проблем обусловлена низким уровнем знаний сотрудников о различных аспектах информационной безопасности, а также недостаточным вниманием к вопросам безопасности со стороны как персонала, так и администрации. Необходимо разъяснять сотрудникам ценность той информации, с которой они работают, и объяснять им, почему медицинские данные требуют защиты, обеспечиваемой IT-специалистом и/или системным администратором. Благо сейчас есть большое количество инструментов, которые помогают предотвратить значительное число угроз, но важно помнить и разъяснять, что компьютер – это только среда, безопасность которой зависит от человеческого фактора.

Проведенный аудит также выявил, что для многих паллиативных служб характерны такие проблемы, как отсутствие современного программного обеспечения или обновлений, обеспечивающих противовирусную защиту; несвоевременная смена паролей точек доступа к сети Wi-Fi или использование одинаковых и простых паролей на всех точках доступа; хранение информации о пациентах в слабо защищенных CRM-системах, используемых врачами, или других программах.

4. КОГДА НУЖНО ПРИСТУПАТЬ К РЕШЕНИЮ ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

Краткий ответ на вопрос, вынесенный в заголовок, – думать об информационной безопасности организации в сфере паллиативной помощи детям следует ВСЕГДА: с момента планирования организации и в течение всего периода ее работы.

Информационная безопасность организации должна стать одним из неотъемлемых и рутинных элементов работы любой организации, оказывающей помощь тяжелобольным детям.

На этапе создания организации следует провести оценку рисков.

Для этого необходимо:
1. Определить потенциальные убытки, которые могут грозить вашей организации, в том числе:

- человеческие – риски, с которыми могут столкнуться Ваши благополучатели, волонтеры, сотрудники, партнеры/контрагенты, благотворители;

- финансовые – потеря ресурсов или репутационные риски, связанные с пожертвованиями, грантами, прибылью от коммерческой деятельности и т. п.;

- материальные – утеря или нанесение вреда помещению, оборудованию и прочим активам Вашей организации;

- информационные – полная или частичная утрата баз данных, технологий, информации и т. п.;

- репутационные – небрежное отношение к информационной безопасности несет в себе огромную угрозу утраты репутации Вашей организации как надежного исполнителя услуг, партнера, благополучателя.

Установив потенциальные риски, следует продумать, какие шаги необходимо предпринять для усиления безопасности, что можно сделать, чтобы избежать опасностей. На этом же этапе мы рекомендуем определить не только меры профилактики, но и меры реагирования на случай, если возникнет реальная угроза.

Важным аспектом информационной безопасности в учреждениях/организациях паллиативной помощи детям является документационное сопровождение этой деятельности. После того как вы сформулируете риски и поймете, что с ними делать, следует закрепить это в соответствующих внутренних документах Вашей организации, а именно – необходимо включить вопросы информационной безопасности в корпоративную политику организации, приказы, должностные инструкции, правила внутреннего распорядка и пр.

В дальнейшем важно не просто внедрить меры информационной безопасности, но и регулярно проводить мониторинг новых возникающих рисков и, соответственно, реагировать на них разработкой дополнительных мер.

5. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ

Мы предлагаем следующие принципы защиты данных в информационных системах, актуальные как для бизнеса, так и для общественных, государственных организаций, в том числе оказывающих паллиативную помощь детям:

1. ЗАКОННОСТЬ И ОБОСНОВАННОСТЬ ЗАЩИТЫ.

Принцип законности и обоснованности предусматривает то, что защищаемая информация по своему правовому статусу относится к информации, которой требуется защита в соответствии с законодательством.

2. СИСТЕМНОСТЬ.

Упорядоченный подход к защите информационной системы предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

- при всех видах информационной деятельности и информационного проявления;
- во всех структурных элементах;
- при всех режимах функционирования;
- на всех этапах жизненного цикла;
- с учетом взаимодействия объекта защиты с внешней средой.

При обеспечении безопасности необходимо учитывать все слабые, наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно злоумышленников – высококвалифицированных технических специалистов), пути проникновения в распределенные системы и пути несанкционированного доступа к информации. Система защиты должна строиться не только с учетом

всех известных каналов проникновения, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

3. КОМПЛЕКСНОСТЬ.

Комплексное использование предполагает согласование в применении разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

4. НЕПРЕРЫВНОСТЬ ЗАЩИТЫ.

Защита информации — это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы, начиная с самых ранних стадий проектирования. Разработка комплекса средств защиты должна вестись параллельно с разработкой самой защищаемой системой.

5. РАЗУМНАЯ ДОСТАТОЧНОСТЬ.

Создать абсолютно неуязвимую систему защиты принципиально невозможно: при достаточных средствах и времени можно преодолеть любую защиту. Следовательно, возможно достижение лишь некоторого приемлемого уровня безопасности. Высокоэффективная система защиты требует больших ресурсов (финансовых, материальных, технологических, временных) и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

6. ГИБКОСТЬ.

Внешние условия и требования с течением времени меняются. Принятые меры и установленные средства защиты могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для варьирования уровня защищенности средства защиты должны обладать определенной гибкостью.

7. ОТКРЫТОСТЬ АЛГОРИТМОВ И МЕХАНИЗМОВ ЗАЩИТЫ.

Суть принципа открытости механизмов и алгоритмов защиты состоит в том, что знание алгоритмов работы системы защиты не должно давать возможности ее преодоления даже разработчику защиты. Однако это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна, необходимо обеспечивать защиту от угрозы раскрытия параметров системы.

8. ПРОСТОТА ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения малопонятных ему операций.

6. СРЕДСТВА РЕАЛИЗАЦИИ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрим основные средства, используемые для создания механизмов защиты.

Все средства защиты делятся на формальные (выполняющие защитные функции строго по заранее предусмотренной схеме без непосредственного участия человека) и неформальные (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

Технические средства представляют собой электрические, электромеханические и электронные устройства. Вся совокупность технических средств делится на аппаратные и физические.

Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой через стандартный интерфейс. Физические средства включают в себя автономные устройства и системы. Это могут быть, например, замки на дверях помещений, где размещена аппаратура или носители особо конфиденциальной информации, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Указанные выше средства и составляли основу механизмов защиты на первой фазе развития технологии обеспечения безопасности связи в каналах телекоммуникаций. При этом считалось, что основными средствами защиты являются программные. Практика показала, что надежность подобных

механизмов защиты является явно недостаточной. Особенно слабым звеном оказалась защита с помощью пароля. Поэтому в дальнейшем механизмы защиты становились все более сложными, к ним начали привлекать другие средства обеспечения безопасности.

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы системы на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

Законодательные средства защиты определяются законодательными актами, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере развития техники и средств связи в нашем обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета человека или престижа организации.

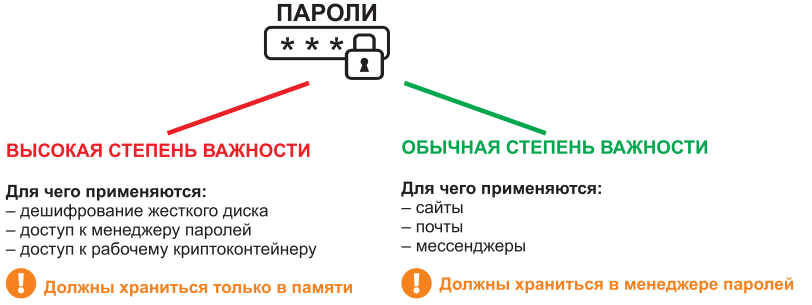
7. ПРОСТЫЕ МЕРЫ ДЛЯ РЕШЕНИЯ СЛОЖНЫХ ПРОБЛЕМ

Пока в организацию не пришел профессиональный специалист, способный системно обеспечить решение вопросов информационной безопасности, мы рекомендуем руководителям и сотрудникам паллиативных служб придерживаться простых правил и внедрять базовые принципы безопасности:

1. НАДЕЖНЫЙ ПАРОЛЬ.

Использование надежных паролей далеко не такой простой вопрос, как может показаться на первый взгляд. И хотя большинство пользователей знают фундаментальные требования к надежному паролю, в повседневной жизни они забывают о них, предпочитая надежному паролю простой и легко запоминающийся.

Самые важные пароли должны быть максимально надежными и фиксироваться только в памяти.



Разберем схему выше. Вся информация на вашем компьютере должна быть зашифрована, и для ее дешифровки вам нужно будет вводить пароль. Это пароль высокой степени важности, его вы храните в памяти. Вы расшифровали жест-

кий диск, все ваши пароли обычной степени важности хранятся в зашифрованном файле ключей менеджера паролей (KeePassXC). Для расшифровки этого файла также используется пароль высокой степени важности.

Теперь поговорим о создании практически очень надежных паролей. «Очень надежных» – потому что рано или поздно можно подобрать любой пароль, но время подбора может занять не одну тысячу лет.

Требования к надежному паролю:

- Это не должны быть слова или фразы.
- Пароль arC2397_1 всегда будет более надежным, нежели car23971.
- Это не должны быть даты, особенно знаковые даты.
- Пароль должен содержать не менее 20 символов.
- Пароль должен включать символы верхнего и нижнего регистра, более одной цифры, специальные символы.
- Этот пароль не должен содержать информацию, связанную с вами: адрес, клички домашних животных, дату рождения, номер телефона, название любимой спортивной команды.

Каждый пароль должен быть уникальным, пароли не должны быть похожими. Ни в коем случае не используйте один и тот же пароль в двух местах.

Придумать надежный пароль, который бы соответствовал всем вышеизложенным требованиям и в то же время был максимально простым для запоминания, – не самая простая задача, но в ваших интересах с ней справиться.

2. ДВОЙНАЯ АУТЕНТИФИКАЦИЯ

Аутентификация – проверка подлинности чего-либо, например, проверка введенного пароля путем сравнивания с указанным при регистрации.

Пароль сегодня – самый популярный инструмент защиты доступа, но даже очень надежный пароль уязвим, а потому многими сервисами и программами предлагается помимо пароля использовать какой-либо инструмент дополнительной защиты.

В целом аутентификация не обязательно должна быть именно двойной, она может быть и тройной: например, сначала вы вводите постоянный пароль, потом получаете СМС с одноразовым паролем, а затем подтверждаете свою личность отпечатком пальца.

Наличие двойной аутентификации зависит от сервиса или используемого программного обеспечения: вы не можете использовать ее там, где она не заложена разработчиком. Да и сама двойная аутентификация бывает различной.

SMS-КОДЫ

SMS-коды – средство дополнительной защиты, подразумевающее отправку СМС с авторизационным кодом на номер, указанный в профиле пользователя. Механизм можно считать довольно надежным, но только в том случае, когда ваш номер неизвестен злоумышленникам. К сожалению, восстановить номер или перехватить СМС сегодня не сложно. Есть разные способы перехвата СМС: восстановление сим-карты, доступ к данным на уровне оператора, взлом устройства, принимающего СМС, использование уязвимостей SS7 или поддельной базовой станции. Необходимо помнить, что СМС – это ненадежно, хотя и лучше, чем отсутствие двойной аутентификации.

По возможности откажитесь от СМС в пользу более надежных способов двойной аутентификации.

EMAIL-КОДЫ

Метод можно назвать вполне надежным только в том случае, если есть доступ к электронной почте с другого устрой-

ства. Если вы авторизуетесь со своего компьютера и на этом же компьютере принимаете email с кодом, смысл двойной аутентификации теряется.

Не принимайте** email-**коды на том же устройстве, с которого осуществляется авторизация.

ТАБЛИЦА С КОДАМИ

Таблица с кодами – способ дополнительной защиты, предусматривающий наличие таблицы с нумерованными кодами, один из которых запрашивается при авторизации. Такую таблицу надо обязательно распечатать, не имеет смысла хранить ее в электронном виде. Это позволит защититься, например, от вредоносного программного обеспечения, которое используется мошенниками для кражи пароля. Злоумышленники могут получить доступ к вашему компьютеру и украсть у вас пароль, но он им ничего не даст, так как для авторизации будет необходимо указать код из таблицы, которой нет на вашем компьютере. К сожалению, пользователи часто не понимают этого и хранят таблицу с кодами в электронном виде. Этим они облегчают мошенникам задачу, фактически сводя на нет двухфакторную аутентификацию.

Распечатайте таблицу с кодами и никогда не храните ее в электронном виде.

3. ЗАЩИТА РОУТЕРА

Так сложилось, что многие несерьезно относятся к защите своей домашней и корпоративной Wi-Fi-сети и самого маршрутизатора. Даже если Wi-Fi-сеть защищают каким-то паролем, заводской пароль маршрутизатора оставляют неизмененным. Очень часто пользователи оставляют Wi-Fi-сеть полностью открытой. По доброте душевной или просто лень устанавливать, а потом еще и вводить этот пароль.

УСТАНОВИТЕ НАДЕЖНЫЙ ПАРОЛЬ WI-FI-СЕТИ

Ваша Wi-Fi-сеть должна быть защищена паролем. Хорошим паролем. Никаких «11111111», «12345678», «qwertyui» и т. д. Не поленитесь придумать надежный пароль, в котором будут заглавные буквы, цифры и специальные знаки (~ ! @ # $ % & *).

Настройки безопасности беспроводной сети – это не только пароль. В настройках необходимо выбрать современный и надежный тип безопасности и шифрования беспроводной сети. Оптимальный выбор защиты – WPA2 – Personal с шифрованием AES.

Защитите настройки маршрутизатора паролем

Этот пароль никак не относится к Wi-Fi. Он используется исключительно для защиты настроек роутера. Чтобы никто, кроме вас, не смог зайти в веб-интерфейс роутера и сменить там какие-то настройки. Как правило, устанавливается логин и пароль (иногда только пароль). На некоторых роутерах он установлен по умолчанию. Обычно используется admin/admin. Если по умолчанию пароль не установлен, то в процессе первой настройки роутер предлагает установить его. Но это в любой момент можно сделать на панели управления.

Отключите функцию WPS

С помощью WPS можно быстро и без ввода пароля подключать устройства к беспроводной сети. Но, как показывает практика, WPS мало кто пользуется. Можно найти много материалов, где говорится о разных проблемах с безопасностью функции WPS. Поэтому, для защиты роутера от взлома, эту функцию лучше отключить.

Кроме этого, из-за WPS очень часто не удается подключить некоторые устройства к Wi-Fi или настроить маршрутизатор в режиме моста.

Спрячьте Wi-Fi-сеть от посторонних глаз

В настройках Wi-Fi-сети на маршрутизаторе есть такая функция как «Скрыть SSID» (Hide SSID), или «Отключить широковещание SSID». После ее активации устройства перестанут видеть вашу Wi-Fi-сеть. А чтобы к ней подключиться, нужно будет указать не только пароль, но и имя самой сети (SSID). А это дополнительная защита.

Эта настройка обычно находится в разделе с настройками беспроводной сети. Можете посмотреть, например, как сделать Wi-Fi-сеть невидимой на роутерах TP-Link.

4. ОПАСНЫЕ ФЛЕШКИ

Классифицируем угрозы, которые могут исходить от флешки или иного USB-носителя, например внешнего жесткого диска.

Первое – это вредоносное программное обеспечение, записанное на флешку с целью заразить компьютер жертвы. Об этой угрозе знает большинство читателей. Однако автозапуск файлов сегодня блокируют практически все операционные системы и тем более антивирусы, потому простое открытие флешки с трояном в большинстве ситуаций неопасно.

Современные устройства достаточно хорошо защищены от заражения вредоносным программным обеспечением путем его автоматического запуска без участия пользователя, но все же не стоит рисковать своим ПК.

Второе – это флешки, на которых размещены сами по себе безопасные файлы, цель которых – привести пользователя на сайт злоумышленника.

Третье – это мошенничество. Например, на флешке могут оказаться доступы к интернет-банку с тысячами долларов на счету.

Флешка может оказаться и USB-киллером, способным вывести из строя компьютер жертвы – это четвертый вариант атаки. Если вы вставите в свой компьютер такую флешку, готовьтесь к покупке новой материнской платы.

Вероятно, вы не раз столкнетесь с мнением, что любую USB-флешку можно спокойно запускать, если ты умеешь открывать файлы в песочнице (Sandboxie – песочница, или изолированная среда для безопасного запуска программ. Прим. ред.). Расскажите этим экспертам о данной угрозе.

Пятый вариант – BadUSB. На наш взгляд, это самый опасный способ атаки. В данном случае флешка выдает себя за другое устройство, подключаемое через USB.

Шестой вариант – флешка-жучок, которая не наносит вреда компьютеру, разве что заряжается от него, но используется как микрофон для прослушки периметра и/или как GPS-трекер для отслеживания местоположения. Подобные устройства можно легко купить, и с помощью такой флешки можно шпионить за кем угодно.

Никогда и ни при каких обстоятельствах не используйте найденные чужие флешки.

Делать исключение не стоит даже для флешек, полученных от людей, которым вы доверяете. Многие популярные вредоносные программы умеют самостоятельно записывать себя на внешние носители информации, подключаемые к скомпрометированному устройству, таким образом заражая все новые компьютеры.

Не доверяйте даже флешкам, полученным от доверенных лиц.

Есть еще одна адресная атака, которая обычно применяется против руководителей организаций и о которой вам стоит знать. У многих из нас есть USB-флешки, и большинство из

них – стандартные модели, которые каждый может приобрести в магазине.

Злоумышленник, например коллега, выясняет, какую флешку использует жертва, и приобретает аналогичную. На нее записывается вредоносная программа, которая называется именем производителя флешки, например Kingston. Для программы используется ярлык в виде папки, и жертва думает, что это папка, хотя на самом деле это исполняемый файл.

Вставив флешку, жертва не обнаруживает файлов, зато видит «папку» Kingston, которую непременно попытается открыть. В этом случае система уведомит о попытке запуска приложения, которое может называться Kingston security update. Оно будет подписано не связанным с Kingston разработчиком, и никто этого не заметит.

После этого жертве будет сообщено, что это важные обновления, установка которых необходима для дальнейшего использования продукта. В процессе установки у жертвы будут запрошены права администратора, после чего на рабочем столе появится ярлык программы «Kingston Update», а флешка будет очищена.

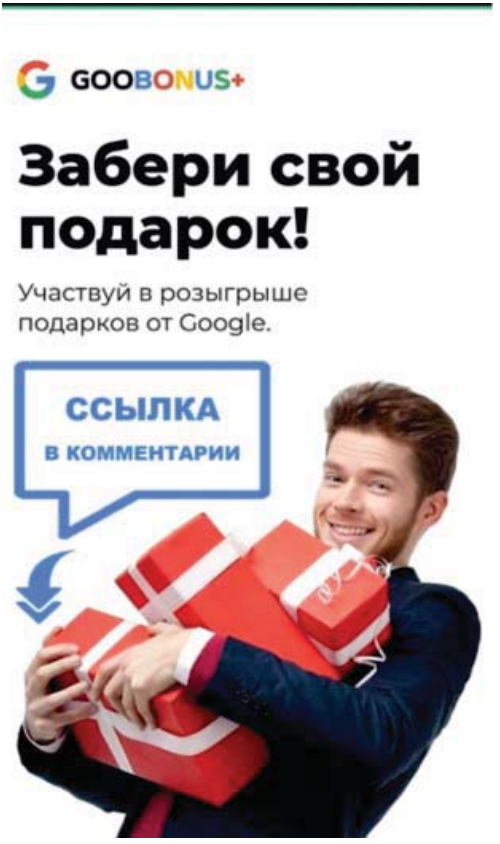
Жертва, скорее всего, удалит установленную программу, проверит ее на вирусы. Но антивирусам придраться будет не к чему, программа служит только для отвлечения внимания и не представляет никакой угрозы. Настоящая угроза уже тайно установлена в систему с правами администратора, и это дает атакующему фактически неограниченную власть над устройством жертвы.

Не недооценивайте угрозу, исходящую от USB-носителей информации, и это не только флешки, но и внешние жесткие диски. Постарайтесь вообще не подключать чужие носители к своему компьютеру, это лучшая защита.

5. ФИШИНГ И ЗАЩИТА ОТ НЕГО

Фишинг – это вид интернет-мошенничества, построенный на принципах социальной инженерии. Главная цель фишинга – получить доступ к критически важным данным (например, паспортным), учетным записям, банковским реквизитам, закрытой служебной информации, чтобы использовать их в дальнейшем для кражи денежных средств. Работает фишинг через перенаправление пользователей на поддельные сетевые ресурсы, являющиеся полной имитацией настоящих.

Классический фишинг – фишинг подмены



К этой категории можно отнести большую часть всех фишинговых атак. Злоумышленники рассылают электронные письма от имени реально существующей компании с целью завладеть учетными данными пользователей и получить контроль над их личными или служебными аккаунтами. Вы можете получить фишинговое письмо от имени платежной системы или банка, службы доставки, интернет-магазина, социальной сети, налоговой и т.д.

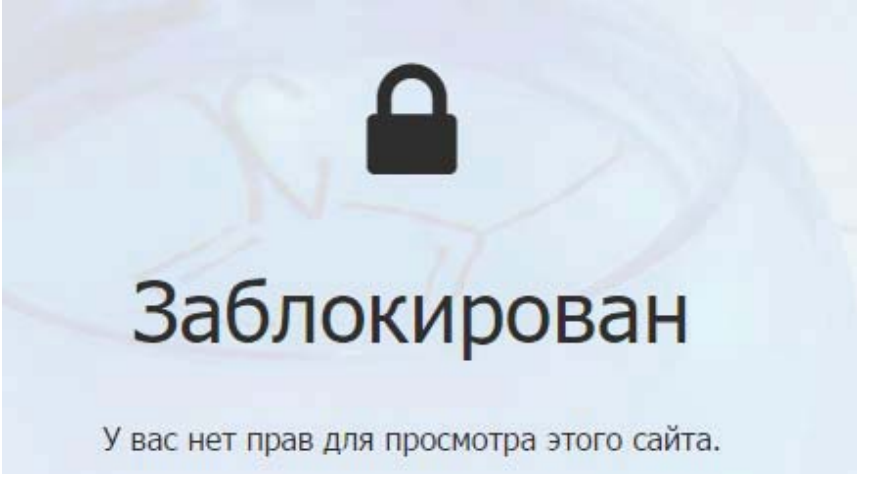
Фишинговые письма создают с большой скрупулезностью. Они практически ничем не отличаются от тех писем, которые пользователь регулярно получает в рассылках от настоящей компании. Единственное, что может насторожить, – просьба перейти по ссылке для выполнения какого-либо действия. Переход этот однако ведет на сайт мошенников, являющийся «близнецом» страницы сайта банка, социальной сети или другого легального ресурса.

Побудительным мотивом для перехода по ссылке в подобных письмах может выступать как «пряник» («Вы можете получить 70% скидку на услуги, если зарегистрируетесь в течение суток»), так и «кнут» («Ваша учетная запись заблокирована в связи с подозрительной активностью. Чтобы подтвердить, что вы владелец аккаунта, перейдите по ссылке»).

Примеры фишинга:

ВАША УЧЕТНАЯ ЗАПИСЬ БЫЛА ИЛИ БУДЕТ ЗАБЛОКИРОВАНА /ОТКЛЮЧЕНА.

Тактика запугивания пользователя может быть очень эффективной. Угроза того, что аккаунт был или в ближайшее время будет заблокирован, если пользователь сейчас же не зайдет в учетную запись, заставляет тут же потерять бдительность, перейти по ссылке в письме и ввести свой логин и пароль.



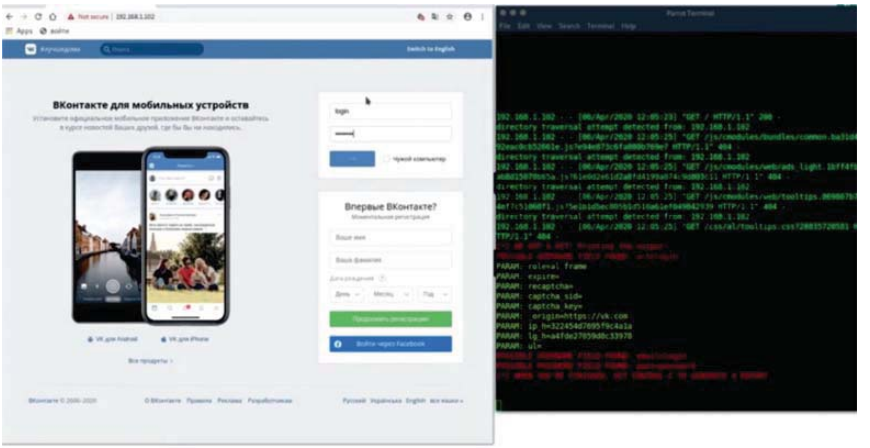
В ВАШЕЙ УЧЕТНОЙ ЗАПИСИ ОБНАРУЖЕНЫ ПОДОЗРИТЕЛЬНЫЕ ИЛИ МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ. ТРЕБУЕТСЯ ОБНОВЛЕНИЕ НАСТРОЕК БЕЗОПАСНОСТИ.

В таком письме пользователя просят срочно войти в учетную запись и обновить настройки безопасности. Действует тот же принцип, что и в предыдущем пункте. Пользователь паникует и забывает о бдительности.

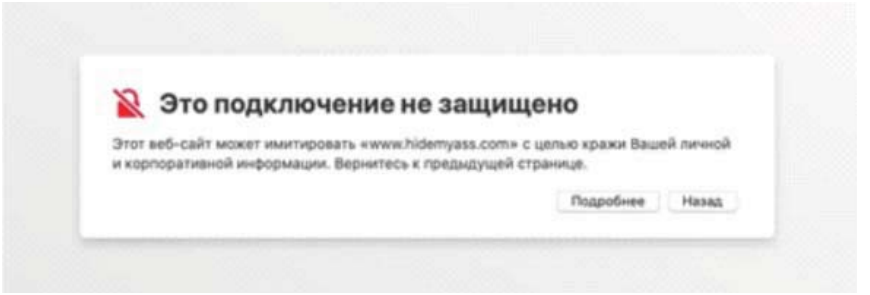
ВЫ ПОЛУЧИЛИ ВАЖНОЕ СООБЩЕНИЕ. ПЕРЕЙДИТЕ В ЛИЧНЫЙ КАБИНЕТ, ЧТОБЫ ОЗНАКОМИТЬСЯ.

Чаще всего такие письма присылают от имени финансовых организаций. Пользователи склонны верить правдивости писем, поскольку финансовые организации действительно не пересылают конфиденциальную информацию по электронной почте.

ФИШИНГОВЫЕ ПИСЬМА НАЛОГОВОЙ ТЕМАТИКИ.
Такие письма входят в тренд, как только близится время платить налоги. Темы писем могут быть самыми разными: уведомление о задолженности, просьба выслать недостающий документ, уведомление о праве на получение возврата налога и т.д.



На данном рисунке изображены два экрана: первый экран – поддельная страница авторизации в популярной социальной сети, которая открылась у «жертвы». Второе окно – у злоумышленника, в котором он видит логин с паролем от входа в личный профиль, которые ввел человек, перейдя по фишинговой ссылке.



Типичное предупреждение от браузера, которое не стоит игнорировать. Получив такое предупреждение, обязательно проверьте в строке ввода адреса сайта его название, которое должно совпадать с тем, куда вы пытаетесь зайти.

Защита от фишинга – основные правила

1. Обязательно проверить URL-адрес, по которому рекомендуется перейти, на наличие незначительных ошибок в написании.
2. Использовать лишь безопасные https-соединения. Отсутствие всего одной буквы "s" в адресе сайта должно насторожить.
3. С подозрением относиться к любым письмам с вложениями и ссылками. Даже если они пришли со знакомого адреса, это не дает гарантии безопасности: он мог быть взломан.
4. Получив неожиданное подозрительное письмо, стоит связаться с отправителем каким-либо альтернативным способом и уточнить, он ли послал сообщение.
5. Если все же необходимо посетить ресурс, лучше ввести его адрес вручную или воспользоваться ранее сохраненными закладками (увы, от фарминга это не убережет).
6. Не использовать для доступа к онлайн-банкингу и другим финансовым сервисам открытые Wi-Fi-сети: часто их создают злоумышленники. Даже если сеть оригинальна, подключиться к незащищенному соединению не составляет сложности для хакеров.
7. На всех аккаунтах, где это возможно, подключить двухфакторную аутентификацию. Эта мера может спасти положение, если основной пароль стал известен взломщикам.

ИСПОЛЬЗОВАНИЕ VPN

Более половины популярных бесплатных VPN-приложений имеют связь с Китаем, где интернет жестко контролируется.

Почти 60% самых популярных бесплатных VPN-приложений в Google Play Store и Apple App Store созданы китайскими разработчиками или принадлежат владельцам из Китая. Об этом сообщается в отчете компании Metric Labs.

«Как показало наше исследование, более половины самых популярных бесплатных VPN-приложений или принадлежат китайцам, или были созданы в Китае, где за последний год усилилось давление на VPN-сервисы, а интернет жестко контролируется», – сообщил глава исследовательского отдела Metric Labs.

В ходе исследования специалисты изучили первую двадцатку бесплатных VPN-приложений из поисковой выдачи Google Play Store и Apple App Store в США и Великобритании. У 17 из 30 приложений (10 приложений были в обоих магазинах) исследователи обнаружили юридическую связь с Китаем – они либо были зарегистрированы в КНР, либо принадлежали китайским владельцам.

У большинства проанализированных приложений практически отсутствует юридически закрепленная защита приватности и поддержка пользователей. У 86% сервисов политика конфиденциальности является «неприемлемой». К примеру, в некоторых не уточняется, регистрируется ли трафик, а некоторые сформулированы лишь в общих чертах даже без упоминания слова VPN.

В ряде приложений политика конфиденциальности и вовсе отсутствует. Более того, в пользовательских соглашениях нескольких приложений прописано, что они обмениваются данными с третьими сторонами, отслеживают пользователей и отправляют данные в Китай.

Ваши личные данные, которые «шифруются» подобными приложениями, могут попасть не в те руки. Приватностью и анонимностью это назвать сложно, так как функционал напоминает *proxy-сервер (простая подмена ip)*.

Почти у половины исследованных приложений политика конфиденциальности размещена в текстовых файлах на Pastebin, серверах AWS или IP-адресах без указания доменного имени. У 64% сервисов отсутствует сайт, а работа осуществляется непосредственно из магазина приложений.

8. ИНФОРМАЦИОННОЕ ВОЛОНТЕРСТВО КАК РЕСУРС ДЛЯ НКО

Сегодня уже ни у кого не вызывает сомнений ценность, эффективность и незаменимость волонтерства в решении самых разных социальных проблем. В паллиативной помощи детям добровольчество стало неотъемлемым элементом профессиональной работы, обеспечивающим высокое качество жизни детей с тяжелыми заболеваниями.

Вместе с тем практика показывает, что даже организации паллиативной помощи детям, в которых уровень развития волонтерских программ довольно высок, зачастую недооценивают возможности информационного или киберволонтерства.

Добровольческие инициативы в интернет-пространстве находятся на этапе развития, поэтому остановимся подробнее на задачах, которые способно решить информационное волонтерство.

Спектр задач информационных волонтеров в контексте паллиативной помощи детям очень широк. Это и преодоление общественных стереотипов в отношении тяжелобольных детей, и распространение информации о возможностях получения помощи, и продвижение философии паллиативной помощи, и консультирование детей и родителей в вопросах безопасного использования интернета и социальных сетей…

Не следует забывать, что для пациентов паллиативных служб интернет служит не только источником информации. Для детей с тяжелыми заболеваниями, находящихся в детском хосписе или дома, интернет играет важную роль, помогая в социализации, обеспечивая возможность общения, дружбы и развития. Именно этот факт делает пациентов пал-

лиативных организаций особенно уязвимыми перед лицом угроз и рисков, с которыми сопряжены современные интернет-коммуникации. Поэтому для специалистов паллиативной помощи так важно понимание интернет-рисков и умение идентифицировать и предотвратить опасности современного виртуального пространства. В этом огромную помощь могут оказать информационные волонтеры.

Опыт Детского хосписа Санкт-Петербурга показывает, что результативность программы информационного волонтерства зависит от ряда факторов:

1. Подготовка информационных волонтеров.

«Школа волонтера» является понятной и привычной ступенькой для всех, кто хочет бескорыстно помогать тяжелобольным детям и семьям, столкнувшимся с неизлечимым заболеванием ребенка. Если паллиативные службы не допускают к общению с детьми людей без специальной подготовки, то ровно такой же подход должен применяться к информационному волонтерству. Влияние информационного волонтера и степень его погруженности в личную историю подопечных может быть очень велика.

2. Наличие информационных волонтеров не отменяет необходимость мер безопасности интернет-пространства, обеспечиваемых со стороны организации паллиативной помощи, таких, например, как обновление программного обеспечения, контроль настроек роутера, антивирусная защита, своевременное обучение сотрудников по вопросам интернет-безопасности.

3. Грамотная организация документационного и организационного сопровождения программ информационного волонтерства.

Несмотря на то что информационное волонтерство пока не относится к областям, жестко регулируемым законодательством, наш опыт показывает, что заключение договоров о волонтерской деятельности в хосписе, неукоснительное

требование не только соблюдения законодательства в отношении персональных данных, но и этического кодекса волонтера обеспечивают первичную защиту прав подопечных организации паллиативной помощи.

4. Оценка и профилактика рисков информационного волонтерства.

Информационное волонтерство в паллиативной помощи связано с доступом к персональной информации и медицинским сведениям, поэтому крайне важно контролировать данное направление и проводить регулярный мониторинг информационного пространства. Как правило, данная обязанность ложится на координатора волонтерских программ.

В заключение хотелось бы добавить, что параллельно с развитием паллиативной помощи в России развивается и рынок IT- и информационной безопасности. Многие компании, профессионально работающие в области информационной безопасности, постепенно приходят к пониманию необходимости развития корпоративной социальной ответственности. Мы рекомендуем рассматривать IT и IB компании как перспективный ресурс для развития собственных программ информационного волонтерства.

ГЛОССАРИЙ

Основные термины и определения правовых понятий в области информационных отношений и защиты информации

Основные термины и определения правовых понятий в изучаемой области установлены в Федеральном законе «Об информации, информационных технологиях и о защите информации».

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – комплекс, включающий вычислительное (компьютеры, серверы, микрокомпьютеры) и коммуникационное оборудование (точки доступа Wi-Fi, маршрутизаторы, концентраторы, кабели), программное обеспечение (операционные системы, приложения для различных задач) и информационные ресурсы, а также системный персонал, обеспечивающий поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Также к правовым понятиям следует отнести понятие прав доступа к защищаемой информации. Ограничения доступа устанавливаются к сведениям, составляющим государственную тайну и иные виды тайны. В качестве собственников информации рассматриваются государство, организации и граждане (юридические и физические лица).

Доступ к информации – возможность получения информации и ее использования.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации – принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2) соблюдение конфиденциальности информации ограниченного доступа;
3) реализацию права на доступ к информации.

Защита информации от утечки – деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Защита информации от несанкционированного воздействия – деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения – деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может быть: государство; юридическое лицо; группа физических

лиц, в том числе общественная организация; отдельное физическое лицо.

Защита информации от разведки – деятельность, направленная на предотвращение получения защищаемой информации разведкой.

Примечание. Получение защищаемой информации может быть осуществлено как иностранной, так и отечественной разведкой.

Защита информации от технической разведки – деятельность, направленная на предотвращение получения защищаемой информации разведкой с помощью технических средств.

Защита информации от агентурной разведки – деятельность, направленная на предотвращение получения защищаемой информации агентурной разведкой.

Цель защиты информации – заранее намеченный результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации (или) несанкционированного и непреднамеренного воздействия на информацию.

Замысел защиты информации – основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации.

Нормы эффективности защиты информации – значения показателей эффективности защиты информации, установленные нормативными документами.

Организация защиты информации – содержание и порядок действий, направленных на обеспечение защиты информации.

Система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Мероприятие по защите информации – совокупность действий, направленных на разработку и (или) практическое применение способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации – совокупность действий, направленных на разработку (или) практическое применение способов и средств контроля эффективности защиты информации.

Техника защиты информации – средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Объект защиты информации – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Категорирование защищаемой информации (объекта защиты) – установление градации важности защищаемой информации (объекта защиты).

Контроль состояния защиты информации – проверка соответствия организации и эффективности защиты информации установленным требованиям и (или) нормам зашиты информации.

САНКТ-ПЕТЕРБУРГ ДЕТСКИЙ ХОСПИС

Читайте и скачивайте бесплатно другие публикации

Санкт-Петербургского Детского хосписа на сайте

www.детскийхоспис.рф

в разделе «Методические пособия»

Вопросы, на которые мы не знаем ответов. Пособие, предназначенное для специалистов, работающих в условиях многоконфессионального общества, посвящено духовной поддержке детей с тяжелыми заболеваниями и их семей. Духовная поддержка является неотъемлемой частью паллиативной помощи, поэтому священнослужители могут рассматриваться как специалисты паллиативной педиатрии, способные оказать существенное влияние на качество жизни неизлечимо больного ребенка, его семьи и ускорить процесс реабилитации родственников после утраты ребенка. Представленная книга содержит ответы авторитетных представителей традиционных конфессий – христианства, ислама, иудаизма и буддизма – на вопросы, возникающие у специалистов и родителей, столкнувшихся с проблемой неизлечимого заболевания ребенка.

Вопросы, непонятные даже ежу. Книга представляет собой компиляцию, саммари, произведения «Вопросы, на которые мы не знаем ответов»: размышления представителей четырех конфессий – христианства, ислама, иудаизма и буддизма – о вопросах, ответы на которые дать очень сложно. Вместе с ежом, которому страшно, что он ничего не знает, на страницах пытаются понять, почему люди болеют, а особенно, почему болеют дети. Брошюра написана просто и понятно для детей. Однако написанное рассчитано не только на юную аудиторию. Взрослые, посмотрев на вопросы глазами ребенка, смогут по-другому взглянуть на привычные вещи и тем самым найти ответы на волнующие вопросы.

Духовная поддержка семей, столкнувшихся с неизлечимым заболеванием ребенка. В издании описаны общие принципы как справиться с той или иной сложной ситуацией на основе опыта ежедневной практики оказания помощи тяжелобольным детям и их семьям. Рассматривается суть феномена «духовность» с позиций не только религиозного, но и светского мировоззрения. Описываются место духовной поддержки в контексте целей и задач паллиативной помощи и ее основные функции, дается характеристика духовных потребностей неизлечимо больного ребенка и членов его семьи. Отдельное внимание уделяется негативным последствиям, к которым может привести дефицит духовной поддержки. И, конечно же, часть книги посвящена существующим средствам оказания духовной поддержки неизлечимо больным детям и их близким.

Волонтерская деятельность в практике паллиативной помощи детям. В пособии описан опыт работы Санкт-Петербургского Детского хосписа с волонтерами, роль в функционировании организации, людей, готовых безвозмездно и от всего сердца помогать тяжелобольным детям. Для руководства хосписа важными будут подсказки, где найти волонтера, как координировать его работу, какими ресурсами должно обладать учреждение для успешного взаимодействия. Волонтеры в свою очередь почерпнут много ценной информации о правовой стороне своей деятельности и поймут, какими знаниями должны обладать, чтобы стать частью хосписа.

Фандрайзинг для благотворительности. Практическая этика и организационные аспекты. В книгах описаны основные понятия, принципы и инструменты фандрайзинга и коммуникаций для фандрайзинга по взаимодействию с жертвователями и благополучателями. Описано, как выстроить работу по фандрайзингу, в чем особенности этого вида деятельности, каковы объективные требования к ее организации и как ее, эту деятельность, эффективно интегрировать институционально. Предлагаются «подсказки», как искать фандрайзера для организации и какими профессиональными и личными качествами он должен обладать. Интересная особенность книги в том, что авторы при описании каких-либо ситуаций не ограничиваются российскими реалиями, а стараются учитывать богатый международный опыт.

Профилактика профессионального выгорания сотрудников детского хосписа. Методическое пособие адресовано сотрудникам медицинских учреждений, оказывающих паллиативную помощь детям. В нем рассматриваются проблемы подготовки и мотивации персонала детского хосписа, факторы, способствующие возникновению синдрома эмоционального выгорания, стадии его развития и способы профилактики. Работа с детьми с тяжелыми заболеваниями связана с крайне высокой степенью ответственности и требует от персонала огромных эмоциональных затрат, в связи с чем осуществление профилактики профессионального выгорания сотрудников детских хосписов представляется необходимым.

Для заметок:

Для заметок:

197229, Санкт-Петербург,
Коннолахтинский проспект, дом 23А

www.детскийхоспис.рф
info@kidshospice.org

Телефон:
+7 (812) 416-13-30
Автономная некоммерческая организация
«Детский хоспис»

ИНН 7814658786
КПП 781401001
ОГРН 1167800053618
ПАО "Банк "Санкт-Петербург" в Санкт-Петербурге
Р/счет 40703810827000003920
К/счет 30101810900000000790
БИК 044030790

Данное издание подготовлено
в рамках проекта
**«Развитие цифровых и дистанционных услуг
в паллиативной помощи детям»**
при поддержке

ФОНД
ПРЕЗИДЕНТСКИХ
ГРАНТОВ

Распространяется бесплатно


9 785906 804099