МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т X.1207

(04/2008)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность электросвязи

Руководящие принципы решения проблемы риска проникновения шпионского ПО и потенциально нежелательного ПО, предназначенные для поставщиков услуг электросвязи

Рекомендация МСЭ-Т X.1207

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	
Службы и услуги	X.1–X.19
Интерфейсы	X.20–X.49
Передача, сигнализация и коммутация	X.50–X.89
Сетевые аспекты	X.90–X.149
Техническое обслуживание	X.150–X.179
Административные предписания	X.180–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	
Модель и обозначение	X.200–X.209
Определения служб	X.210–X.219
Спецификации протоколов с установлением соединений	X.220–X.229
Спецификации протоколов без установления соединений	X.230–X.239
Проформы PICS	X.240–X.259
Идентификация протоколов	X.260–X.269
Протоколы обеспечения безопасности	X.270–X.279
Управляемые объекты уровня	X.280–X.289
Испытание на соответствие	X.290–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	
Общие положения	X.300–X.349
Спутниковые системы передачи данных	X.350–X.369
Сети, основанные на протоколе Интернет	X.370–X.379
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	
Организация сети	X.600–X.629
Эффективность	X.630–X.639
Качество обслуживания	X.640–X.649
Наименование, адресация и регистрация	X.650–X.679
Абстрактно-синтаксическая нотация 1 (ASN.1)	X.680–X.699
УПРАВЛЕНИЕ В ВОС	
Структура и архитектура управления системами	X.700–X.709
Служба и протокол связи для общего управления	X.710–X.719
Структура управляющей информации	X.720–X.729
Функции общего управления и функции ODMA	X.730–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	
Фиксация, параллельность и восстановление	X.850–X.859
Обработка транзакций	X.860–X.879
Удаленные операции	X.880–X.889
Общие приложения ASN.1	X.890–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ЭЛЕКТРОСВЯЗИ	**X.1000–**

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1207

Руководящие принципы решения проблемы риска проникновения шпионского ПО и потенциально нежелательного ПО, предназначенные для поставщиков услуг электросвязи

Резюме

В Рекомендации МСЭ-Т X.1207 представлены руководящие принципы решения проблемы риска проникновения шпионского и потенциально нежелательного ПО, предназначенные для поставщиков услуг электросвязи (TSP). В Рекомендации предлагается для внедрения передовой опыт, в основе которого применение ясных по содержанию извещений и обеспечение для пользователя возможности выдачи разрешений, а также функций управления в рамках предоставляемых TSP услуг веб-хостинга. В Рекомендации представлены и предлагаются для внедрения образцы передового опыта для пользователей по обеспечению защиты персонального компьютера (ПК), включая применение программ обнаружения и обезвреживания шпионского ПО и вирусов, применение персональных брандмауэров и программ обновления защитных средств в клиентских системах.

Источник

Рекомендация МСЭ-Т X.1207 утверждена 18 апреля 2008 года 17-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

Ключевые слова

Вводящее в заблуждение ПО, безопасность интернета, потенциально нежелательное ПО, шпионское ПО

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1207

Руководящие принципы решения проблемы риска проникновения шпионского ПО и потенциально нежелательного ПО, предназначенные для поставщиков услуг электросвязи

1 Сфера применения

Настоящая Рекомендация являются частью комплекса руководств, разработанных МСЭ-Т в целях повышения уровня кибербезопасности в интернете. Они охватывают требования к базовым мерам по обеспечению безопасности и защиты для поставщиков услуг электросвязи (TSP) и конечных пользователей, при этом основное внимание уделяется решению проблемы шпионского и другого потенциально нежелательного ПО, которое может быть вредоносным и/или вводящим в заблуждение. В рамках настоящей Рекомендации термин "поставщики услуг электросвязи (TSP)" означает TSP, предоставляющих связанные с интернетом услуги, в частности услуги веб-хостинга, предпринимательским структурам, и доступ в интернет для конечных пользователей.

2 Справочные документы

Отсутствуют.

3 Определения

Термин "шпионское ПО" используется в широком смысле, с тем чтобы охватить многочисленные формы ПО, характеризующиеся определенными режимами, которые предполагают проникновение в конфиденциальные данные и которые не запрашивались конечными пользователями. Для обеспечения согласованного применения и общего понимания в настоящем документе приводится рабочее определение термина "шпионское ПО" и связанного с ним термина "вводящее в заблуждение ПО".

3.1 Вводящее в заблуждение ПО

Программное обеспечение, которое выполняет действия на компьютере пользователя без: 1) предварительного уведомления пользователя о том, какие именно действия программное обеспечение выполнит на компьютере пользователя; или 2) запроса разрешения пользователя на выполнение этих действий программным обеспечением. К примерам вводящего в заблуждение ПО относятся программы, которые перехватывают пользовательские конфигурации или программы, что приводит к бесконечному появлению на экране рекламы, которую пользователь не может удалить с помощью простых операций.

3.2 потенциально нежелательное ПО: Потенциально нежелательное ПО означает различные формы вводящего в заблуждение программного обеспечения, в том числе вредоносное программное обеспечение, такое как вирусы, черви, троянцы, и невредоносное программное обеспечение, которому присущи свойства вводящего в заблуждение или шпионского ПО.

3.3 шпионское ПО: Шпионское ПО определяется в настоящей Рекомендации как частный случай вводящего в заблуждение ПО, которое выбирает из компьютера пользователя его личные данные. Личные данные могут включать такие сведения, как наиболее часто посещаемые веб-сайты или более ценную информацию, такую как пароли.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

CERT	Computer Emergency Response Team	Группа быстрого реагирования на нарушения компьютерной защиты
CIRT	Computer Incident Response Team	Группа по расследованию компьютерных инцидентов

ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
ISMS	Information Security Management System		Система управления информационной безопасностью
ISMS-T	Information Security Management System – Requirements for Telecommunications		Система управления информационной безопасностью – требования к электросвязи
ISV	Independent Software Vendor		Независимый поставщик программного обеспечения
SQL	Structured Query Language		Структурированный язык запросов
TSP	Telecommunication Service Providers		Поставщики услуг электросвязи
URI	Uniform Resource Identifier		Унифицированный идентификатор ресурса

5 Условные обозначения

Отсутствуют.

6 Обзор

Быстрое распространение интернета открывает возможности создания новых коммерческих предприятий и предоставляет потребителям множество преимуществ в домашних условиях и на рабочих местах. Присущий интернету открытый характер, а также обеспечиваемые им межсетевое взаимодействие и скорость доступа обусловливают превращение интернета в эффективную платформу связи предприятий и потребителей, а также связи для целей массового маркетинга. В последние годы такую открытость и простоту установления связи и подключения все в большей степени используют в своих интересах киберпреступники и мошеннические коммерческие предприятия, применяя для получения финансовой прибыли и других преступных целей различные формы вредоносного программного обеспечения.

Одной из приобретающих все большую значимость проблем безопасности и защиты является шпионское ПО и вводящее в заблуждение ПО, которые могут представлять опасность для личной информации, являться причиной существенного падения эффективности и подрывать доверие конечных пользователей к законным коммерческим предприятиям, функционирующим в интернете.

На поставщиков услуг электросвязи (TSP) полагаются различные стороны, в частности регуляторные органы и корпоративные клиенты, для получения безопасных и защищенных услуг интернета конечными пользователями (включая потребителей и корпоративных пользователей). Если обнаруживается, что размещенные в сетях TSP веб-сайты являются распространителями вредоносного контента, включая шпионское и вводящее в заблуждение ПО, и нарушают безопасность и защиту компьютерных систем конечных пользователей, к TSP обращаются за помощью в решении этих проблем, и любые продолжительные или часто повторяющиеся такие инциденты скажутся на доверии к TSP и уверенности в том, что они предоставляют безопасные и защищенные услуги. Это выразится в неудовлетворенности потребителей, результатом чего станет отток клиентов к другим TSP.

Что касается регуляторного аспекта, во многих странах регуляторные органы все чаще требуют от TSP гарантий в отношении принимаемых ими мер защиты и безопасности, а также расширения деятельности, направленной на содействие потребителям и конечным пользователям в обеспечении безопасности и защиты работы в интернете.

В свете этих изменений, происходящих в режимах безопасности и защиты интернета, для TSP важно принять комплекс базирующихся на передовом опыте стандартов, которые могли бы быть признаны во всей отрасли в качестве минимальной основы[1], обеспечивающей безопасные и защищенные услуги интернета, предоставляемые через TSP, а также распространять соответствующую практику

[1] В настоящее время такой основы не существует, и настоящая Рекомендация, содержащая руководящие принципы, является одним из шагов к обеспечению такой минимальной основы.

среди конечных пользователей, являющихся абонентами их сетей. Внедрение базового стандарта также позволит TSP продемонстрировать регуляторным органам и конечным пользователям свое соответствие передовому опыту отрасли и повысить, если не сохранить, уровень доверия и уверенности регуляторных органов и конечных пользователей в отношении безопасности и защиты сети и услуг TSP.

7 Цели

Целями настоящей Рекомендации являются:

1) внедрение передового опыта, в основе которого применение ясных по содержанию извещений и обеспечение для пользователя возможности выдачи разрешений, а также функций управления в рамках услуг веб-хостинга; и

2) внедрение передового опыта обеспечения защиты (через поставщиков услуг электросвязи) среди работающих в домашних условиях пользователей по безопасному и защищенному использованию персональных компьютеров и интернета, включая применение программ обнаружения и обезвреживания вирусов, шпионского ПО, применение персональных брандмауэров и автоматического обновления защитных средств.

8 Вводящее в заблуждение и шпионское ПО

Общей чертой всех вводящих в заблуждение программ (включая шпионское ПО), которая отличает их от легальных приложений, является отсутствие извещений и возможности выбора на пользовательском уровне. Важным является широко отмечаемый факт, что при надлежащем раскрытии информации, авторизации и контроле со стороны пользователя многие из задач, выполняемых вводящим в заблуждение/шпионским ПО могут приносить пользователям выгоду. Например, такие программы могут способствовать персонификации, позволять вводить утверждаемые пользователем изменения конфигурации и распространять утвержденную рекламу, что, в свою очередь, может "субсидировать" столь высоко ценимую услугу, как электронная почта. Если кратко, вводящее в заблуждение ПО не является преимущественно технической проблемой, но, в основном, проблемой, порождаемой дезориентирующим или мошенническим образом действия.

И на глобальном, и на местном уровнях вводящее в заблуждение ПО и шпионское ПО стали наиболее актуальными проблемами для правительств, отрасли и потребителей и в этом отношении вышли за рамки исключительно вопроса "политики в области ИКТ". Поскольку вводящее в заблуждение ПО очевидно использует интернет и компьютер в качестве своей среды передачи, это, по существу дела, проблема защиты потребителя, которая возникает вследствие вводящих в заблуждение действий.

9 Почему вводящее в заблуждение и шпионское ПО представляют проблему

На уровне потребителей такое ПО отрицательно сказывается на отношении пользователей к работе с применением компьютера и/или в онлайновом режиме (иногда до такой степени, что компьютер представляется бесполезным) и вызывает ощущение неудовлетворенности и "потери контроля". Не будет преувеличением предположить, что значительную долю потребителей составляют бытовые пользователи, для которых вводящее в заблуждение ПО грозит полным уничтожением тех исключительных преимуществ, которые предоставляет интернет и собственно работа с использованием компьютера.

Кроме того, что вводящее в заблуждение ПО оказывает значительное влияние на потребителей, оно представляет серьезную проблему также и для многих занимающихся ИКТ компаний. Единодушно многие клиенты незаслуженно относят проблемы функционирования своего компьютера на счет производителей и поставщиков услуг, что отрицательно сказывается на их репутации и отношении потребителей к их продуктам. Очевидно, что следствием проблем, причиной которых является вводящее в заблуждение ПО, являются миллионы долларов, затрачиваемые на ненужные обращения за поддержкой в обоих секторах – программного и аппаратного обеспечения.

Как указано в разделе 6, выше, TSP причастны к решению проблем, создаваемых шпионским и вводящим в заблуждение ПО, в силу их деятельности по веб-хостингу, который может напрямую использоваться мошенническими предприятиями и киберпреступниками для захвата этих веб-сайтов, а их абоненты, непосредственно испытывая отрицательное воздействие, обращаются к TSP за

получением поддержки и помощи. В довершении всего, регуляторные органы и конечные пользователи ожидают, что TSP принимают адекватные меры по обеспечению безопасности и защиты для борьбы с такими проблемами. Если TSP отказываются от функции разрешения этих проблема, их репутация, а также уверенность и доверие к ним конечных пользователей, естественно, подрываются.

10 Рекомендации

Наиболее эффективным способом противостояния шпионскому ПО является, видимо, сочетание нескольких стратегий с участием различных заинтересованных сторон:

– отраслевой передовой опыт – в сотрудничестве со всеми основными участниками обнаружение и решение проблемы проникновения шпионского и другого нежелательного ПО;

– широкое просвещение потребителей – обеспечение надежного ресурса, содержащего сведения о том, как удалять шпионское и другое нежелательное ПО и избегать его;

– инновационные технологические решения – помощь в защите пользователей от шпионского и другого потенциально нежелательного ПО и поддержание способности противостоять ему; и

– законодательная и правоприменительная деятельность правительства при содействии со стороны отрасли – противодействие разработке вводящего в заблуждение и шпионского ПО.

Настоящие руководящие принципы направлены на распространение передового отраслевого опыта и обеспечение просвещения широких слоев потребителей в помощь TSP при проведении активной деятельности по противодействию вводящему в заблуждение и шпионскому ПО.

11 Руководящие принципы для поставщиков услуг электросвязи (TSP)

В целях содействия решению проблем, связанных с водящим в заблуждение и шпионским ПО, настоящие руководящие принципы охватывают три основные области, а именно: управление системой внутренней безопасности самой организации TSP; требования к мерам по защите, определяемые TSP для своих потребителей услуг веб-хостинга как обязательные для внедрения; и руководящие принципы, полезные для конечных пользователей (или абонентов) услуг доступа в интернет. Рекомендации сгруппированы по трем соответствующим подразделам следующим образом:

a) управление рисками нарушения информационной безопасности на предприятиях;

b) требования к безопасности и защите для услуг веб-хостинга;

c) руководящие принципы обеспечения безопасности и защиты для конечных пользователей.

11.1 Управление рисками нарушения информационной безопасности на предприятии

11.1.1 Система управления информационной безопасностью

На уровне предприятий должна существовать официальная система управления информационной безопасностью, внедренная в целях выявления рисков нарушения информационной безопасности для деятельности TSP и управления ими. В [b-ITU-T X.1051] содержатся руководящие указания и описание передового опыта, необходимые для реализации такой системы.

Основным фактором, который должны учитывать TSP при внедрении ISMS-T, является обеспечение наличия у TSP, как у предприятия, системы, позволяющей на постоянной основе выявлять, оценивать, интерпретировать риски нарушения информационной безопасности, связанные с предоставляемыми ими интернет-услугами непосредственно конечным пользователям/абонентам и опосредованно – потребителям через услуги веб-хостинга, и управлять этими рисками.

Используя постоянные процессы управления рисками ISMS-T, TSP повысят наглядность своих профилей рисков и смогут демонстрировать регуляторным органам и другим заинтересованным сторонам безопасность своих сетей и услуг.

TSP могут также рассматривать вопрос своей официальной сертификации на соответствие Рекомендациям ISMS-T по системе сертификации ИСО/МЭК 27001.

В качестве части реализации ISMS-T или соответствующей системы управления информационной безопасностью TSP должны также обеспечить возможность мониторинга случаев нарушения безопасности и реагирования на них и координировать свои меры по реагированию с внешними организациями (Группой по расследованию компьютерных инцидентов (CIRT) или Группой быстрого реагирования на нарушения компьютерной защиты (CERT)) в своей стране. Обеспечение быстрого реагирования на инциденты должно включать мониторинг и оценку состояния безопасности конечных пользователей и размещенных в сетях TSP веб-сайтов, а также предоставление руководств в помощь пострадавшим сторонам при организации эффективного реагирования на случаи нарушения безопасности.

11.1.2 Предоставление безопасных и защищенных продуктов

Некоторые TSP могут разрабатывать[2] и внедрять собственные инструменты навигации, номеронабиратели или коды любых типов для предоставления конечным пользователям дополнительных услуг, или упрощения доступа к интернет-услугам. В таком случае должно существовать надлежащее соглашение с конечным пользователем, содержащее соответствующие формулировки и заявления относительно принятой TSP политики кодирования, политики конфиденциальности и средств, с помощью которых пользователи могут впоследствии менять свою позицию в отношении принятия соглашения или направлять вопросы, которые могут возникать относительно принятых политики и практики. Если используется такое соглашение, TSP должен убедиться, что конечные пользователи надлежащим образом подписали его соответствующую версию.

TSP должен также документально оформить режимы работы программы и провести оценку, не возникает ли в ходе работы программы какого-либо режима, в результате которого эта программа может рассматриваться как шпионское или вводящее в заблуждение ПО. В таком случае необходимо привлечь имеющего соответствующую квалификацию эксперта-консультанта, для того чтобы оценить, не соответствует ли эта программа каким-либо объективным критериям поставщиков антишпионского ПО, и следовать образцам передового опыта, так чтобы поставляемые TSP программные инструменты для конечных пользователей не могли быть помечены поставщиками защитного ПО как шпионские/вводящие в заблуждение. Многие поставщики антишпионского ПО публикуют свои критерии классификации ПО[3].

TSP должны внедрять цифровую подпись кода для своих двоичных файлов, так чтобы поставщики антишпионского ПО могли без труда определять владельца файла, а независимые поставщики программного обеспечения (ISV), которые постоянно производят программного обеспечение, отвечающее передовому опыту, классифицировались бы как вероятно безопасные даже до проведения анализа.

Если TSP обнаруживает пригодные программные средства, которые могут способствовать смягчению проблемы шпионского ПО, TSP должен рассматривать вопрос об установлении партнерских отношение и совместной работы с их поставщиком в целях обеспечения широкой доступности этих средств.

11.1.3 Мониторинг сети и ответные меры

Мониторинг сети – это общепринятый среди TSP инструмент обеспечения надежности и качества своих сетевых услуг. В то же время это средство можно эффективно использовать для определения исключительных условий сетевого трафика и выявления злонамеренных действий в сети. В целом TSP должны выполнять следующее:

– различать трафик в сети – какой трафик является нормальным, а какой – анормальным;

– использовать инструмент управления сетью для выявления всплесков трафика, "необычных" трафика/портов и обеспечивать наличие инструментов, позволяющих обнаруживать их причину и принимать ответные меры;

– испытывать функции принятия ответных мер, до того как они потребуются в реальных условиях. Совершенствовать методы, процессы и инструменты принятия ответных мер исходя из результатов регулярных проверок;

---

[2] Либо своими силами, либо с привлечением третьих сторон.

[3] Коалиция против шпионского ПО, объединяющая большое число представителей отрасли, также разработала свод определений и критериев, которые публикуются на ее веб-сайте. Более подробная информация содержится в Дополнении I.

– иметь представление обо всех участниках на индивидуальной основе – если пользователь, обычно являющийся неактивным, неожиданно начинает использовать доступную ширину полосы на 100 процентов, возможно, следует его изолировать до выявления причины такой активности. Сетевая изоляция может предотвращать распространение нарушающих нормальную работу программ (вредоносного ПО), хотя в рамках некоторых реализаций может потребоваться разрешение пользователя или обновление условий обслуживания.

11.1.4 Поддержка и распространение

TSP обычно имеют службу поддержки для ответов на запросы клиентов и обеспечения технической помощи и поддержки для разрешения проблем конечных пользователей. По мере распространения вредоносного ПО в интернете, TSP будут получать сообщения, связанные с проникновением и проблемами вредоносного и шпионского ПО. Такая информация является важной и полезной для соответствующих поставщиков для целей проведения оценки рисков, связанных с вредоносным ПО, и обновления необходимых инструментов, с тем чтобы обеспечивать эффективное удаление или отключение любого нового вредоносного или шпионского ПО. Вследствие этого TSP должны устанавливать связь с поставщиками защитных средств и представлять им соответствующие отчеты и образцы вредоносного ПО для принятия последующих мер, особенно если наблюдается резкое увеличение частоты случаев обнаружения такого ПО. Большинство поставщиков составляют и обновляют список адресов электронной почты для получения таких отчетов/образцов в целях анализа и последующей деятельности. См., например, таблицу I.1.

11.1.5 Информированность о новейших разработках

В качестве части реализации ISMS-T для целей управления рисками нарушения информационной безопасности на предприятии, а также для обеспечения постоянного соответствия TSP передовому отраслевому опыту и готовности к защите с учетом новейших уязвимостей и ситуаций злоупотребления/атак, TSP должны быть участниками соответствующего сообщества или отраслевых форумов, с тем чтобы обмениваться информацией по передовому опыту с коллегами поставщиками.

ПРИМЕЧАНИЕ. – Более подробная информация содержится в Дополнении I.

11.2 Требования к безопасности и защите применительно к услугам веб-хостинга

Большинство TSP предоставляют услуги веб-хостинга в своих сетях и центрах обработки данных в рамках своих услуг для бизнеса. Конечные пользователи/потребители и/или малые предприятия получают эти услуги, когда абоненты услуг веб-хостинга извлекают их из пакета и перепродают конечным пользователям. Если абоненты услуг веб-хостинга создают незащищенный сервер или размещают на своих веб-сайтах вредоносный контент, это весьма негативно сказывается на безопасности и защите конечных потребителей. Вследствие этого для TSP важно ввести для абонентов веб-хостинга минимальный стандарт обеспечения безопасности и защиты на основе передового опыта, соблюдение которого будет предусмотрено условиями соглашения.

Условия соглашения должны охватывать следующее:

a) ясные по содержанию извещения, описывающие принятую практику обеспечения безопасности и конфиденциальности при пользовании веб-сайтом, порядок сбора данных и режимы всех кодов (например, объектов модуля поддержки браузера), которые веб-сайт может распространять на рабочий стол конечного пользователя или в оболочку веб-браузера и выполнять их в этой среде;

b) разрешение пользователя, определяющее согласие или несогласие пользователя с условиями обслуживания, описанными в извещениях. Это обеспечит для пользователя возможность проявлять осторожность и определять, может ли он/она соответствующим образом принять условия обслуживания;

c) средства управления пользователя, дающие пользователям возможность изменять свои установки или иным образом отозвать свое согласие в любое время в будущем после заключения первоначального соглашения.

Эти условия важны для обеспечения информированности конечных пользователей о режимах и принятой практике работы веб-сайта в аспекте безопасности, конфиденциальности и защиты пользователя. Условия обслуживания должны разрабатываться с участием юриста, с тем чтобы они также ограждали TSP от возможных юридических обвинений со стороны конечных пользователей в связи с понесенными ими определенными потерями или ущербом по причине вредоносного контента или нечетко определенной практики, принятой на данном веб-сайте.

Кроме положений о защите данных, конфиденциальности и безопасности на веб-сайте TSP должны требовать внедрения на прикладном уровне размещаемых в их сетях веб-сайтов пакета мер защиты, базирующихся на передовом опыте, до введения этих веб-сайтов в действие. Это должно включать, в том числе, следующее:

a) руководящие указания по практике разработки защищенных веб-сайтов и кодирования веб-страниц, включая:

   i) отображение коротких извещений о конфиденциальности, которые содержат ясное, краткое одностраничное резюме (составленное на понятном широкому кругу читателей языке) принятой компанией обязательной практики обеспечение конфиденциальности в онлайновой среде. В этом случае пользователи могут делать более осознанный выбор относительно помещения своей информации в онлайновую среду. Короткие извещения должны соответствовать всем нормативным требованиям и обеспечивать доступ по ссылке к полным текстам юридических обоснований и другой необходимой информации, так чтобы клиентам, желающим ознакомиться с более подробной информацией, достаточно было щелкнуть по ссылке, чтобы прочитать полный текст. При наличии единого извещения потребители смогут более единообразно пользоваться всеми средствами компании при тех же стандартах обеспечения конфиденциальности и ожидаемых результатах, распространенных на многие сайты;

   ii) защищенную обработку cookie-файлов;

   iii) защищенную проверку и обработку входных данных для предотвращения типичной атаки, такой как "внедрение оператора sql" (SQL-injection);

   iv) защищенное написание сценариев веб-страницы для предотвращения типичной атаки, такой как "межсайтовое выполнение сценариев" (cross-site scripting); и

   v) анализ и испытание безопасности кодов.

В качестве части инфраструктуры веб-хостинга TSP должны приниматься также следующие меры обеспечения безопасности для защиты веб-серверов от несанкционированного доступа и опасности размещения вредоносного контента, такого как вводящее в заблуждение и шпионское ПО:

b) конфигурирование веб-сервера, включая базовые операционные системы, в соответствии с руководством по конфигурации основных элементов системы защиты. Это должно включать надлежащее определение пользователей веб-сервера в сравнении с администратором, внедрение средств управления программными и системными директориями и файлам и разрешение ведения контрольного журнала, в частности для регистрации случаев нарушения безопасности и других случаев отказа в системе;

c) реализация системы, предназначенной для испытания и внедрения обновлений средств защиты, а также для обеспечения своевременной актуализации операционной системы и приложений веб-сервера при появлении новых обновлений средств защиты;

d) мониторинг эффективности защиты веб-сервера путем периодического анализа контрольных журналов;

e) функционирование антивирусного и антишпионского программного обеспечения на сервере;

f) регулярное сканирование всего размещаемого и загружаемого контента с использованием обновленных определений, признавая, что файл может представлять собой шпионское или вводящее в заблуждение ПО, даже если это не выявлено с помощью действующих определений вследствие ограничений, создаваемых неточной информацией;

g) выполнение регулярных тестов на защиту от несанкционированного доступа для веб-сайтов для обеспечения того, что поддерживается адекватный уровень защиты и что он не был нарушен.

Для того чтобы обеспечить возможность контроля этих мер безопасности, особенно мер, касающихся защищенности веб-сревера, TSP должны предусмотреть включение соответствующих положений в соглашения об обслуживании.

11.3 Руководство по обеспечению безопасности и защиты для конечных пользователей

11.3.1 Руководства для пользователей и просвещение пользователей

Следует предоставлять руководства по обеспечению безопасности в онлайновой среде. TSP могут либо непосредственно выпускать руководства, либо обеспечивать пользователей ссылками на доступные сайты, содержащие такие руководства. Очень важное значение имеет просвещение конечных пользователей в вопросах о том, как они могут способствовать безопасности интернета. Примеры кампаний или мероприятий по распространению руководств могут включать следующие:

a) периодический (например, ежемесячный) информационный бюллетень, содержащий рекомендации относительно конкретных методов обеспечения защиты (например, как правильно выбрать пароль), новые данные о тенденциях в области обеспечения безопасности, и извещения об интернет-трансляциях, посвященных безопасности, и других видео-, аудиотрансляциях и информации по безопасности, имеющихся на веб-порталах TSP или других поставщиков контента по обеспечению безопасности;

b) непосредственная трансляция по запросу учебных видеоматериалов по безопасности и/или веб-трансляции по разнообразным вопросам безопасности, предназначенные для освоения конечными пользователями методов защиты и повышения уровня их осведомленности о таких методах;

c) включение посвященной безопасности колонки в информационные бюллетени TSP, подготавливаемые в бумажном виде, которые рассылаются по домашним или рабочим адресам конечных пользователей, с тем чтобы привлечь внимание к основным событиям или информации по безопасности; и

d) ежегодные и другие периодические семинары или выездные презентации по безопасности для конечных пользователей, возможно, в партнерстве с другими участниками отрасли, поставщиками и государственными органами.

11.3.2 Технические меры обеспечения безопасности для конечных пользователей

В рамках просвещения пользователей и обеспечения их руководствами по защите от вводящего в заблуждение и шпионского ПО TSP должны консультировать конечных пользователей по вопросам о применении подходящих технических мер обеспечения безопасности, направленных на защиту своих систем от известных вторжений и атак. Минимальные защитные меры должны включать:

a) использование новейших операционных систем с установленными модулями коррекции системы защиты;

b) использование антивирусных и антишпионских инструментов. По возможности TSP должны устанавливать партнерские отношения с заслуживающими доверия поставщиками средств защиты[4], с тем чтобы предлагать эти средства как часть пакета услуг по подписке, так чтобы средства защиты становились доступными по приобретении абонемента, либо по его обновлении;

c) включение блокировки всплывающих окон (pop-up blocker). Стандартные веб-браузеры и панели инструментов веб-браузеров в настоящее время оборудованы этой функцией, которая предотвращает показ вредоносными веб-сайтами окон со шпионским или вводящим в заблуждение ПО, способным воспользоваться уязвимостью системы или браузера или применить средства психологического воздействия, с тем чтобы обманным путем вынудить пользователей загрузить и установить такое ПО на своих системах. Следует составлять и предлагать список рекомендованных средств блокировки всплывающих окон, а также поощрять их использование, сопровождая такой список руководствами по их включению в работу и способам разрешения отображения всплывающих окон веб-сайтов, получивших разрешение пользователя;

d) включение персональных брандмауэров. Персональный брандмауэр является еще одним важным инструментом контроля сетевых услуг, получающих доступ к пользовательским системам, и наоборот. В ряде новейших операционных систем персональные брандмауэры являются встроенными. По умолчанию брандмауэры включены, однако пользователи или приложения могут отключать их, создавая нежелательный риск нарушения безопасности.

---

[4] Заслуживающими доверия поставщиками средств обеспечения безопасности могут быть коммерческие партнеры TSP и/или поставщики, которые предоставляют продукты и услуги, прошедшие проверку на соответствие политике и требованиям TSP в отношении обеспечения безопасности.

TSP должны содействовать использованию функций персонального брандмауэра и/или предлагать персональные брандмауэры третьей стороны, продукты которых TSP оценивает как заслуживающие доверия, а также просвещать пользователей и оказывать им помощь в обеспечении базовой сетевой безопасности на уровне системы конечного пользователя;

e) разрешение автоматических обновлений. Хотя описанные выше технические средства обеспечения безопасности способны противостоять большинству вредоносного ПО на своих соответствующих операционных уровнях, они не достаточно эффективны в случаях использования уязвимостей, которые существуют в операционных системах и прикладных продуктах. Для предотвращения такого использования предусмотренные в операционной системе функции обновления, которые также обеспечиваются заслуживающими доверие пользователей приложениями (например, антишпионские и антивирусные продукты, оценку которых провела пользующаяся доверием третья сторона), должны быть включены для разрешения выполнения автоматических обновлений. Таким образом будет обеспечиваться обновление систем с помощью новейших модулей коррекции системы защиты, где бы они ни находились, сокращая тем самым временной период, в течение которого могло бы иметь место использование уязвимостей.

В Дополнении I к настоящей Рекомендации содержится перечень ссылок и онлайновых ресурсов, которые можно использовать для поддержки выполнения изложенных выше рекомендаций.

Дополнение I

Дополнительные ресурсы

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

I.1 Онлайновые источники информации по обеспечению безопасности и антишпионскому ПО

Существует ряд веб-сайтов, к которым можно обращаться и которые можно эффективно использовать для получения информации, относящейся к безопасности и защите интернета. К ним относятся:

- **Коалиция против шпионского ПО** (**Anti-spyware Coalition**, http://www.antispywarecoalition.org/) – Группа, созданная для выработки согласованных определений шпионских программ, а также обсуждения передового опыта противодействия шпионскому ПО и другим потенциально нежелательным технологиям. Коалиция, в состав которой входят компании, разрабатывающие антишпионское ПО, научные круги и группы защиты потребителей, стремится свести воедино различные видения проблемы контроля шпионского ПО и других потенциально нежелательных технологий.
- **Be Web Aware** (http://www.bewebaware.ca) – Национальная двуязычная программа публичного образования в области безопасности интернета, целью которой является обеспечение для канадской молодежи возможности использовать преимущества интернета, осуществляя свою деятельность в онлайновой среде в условиях безопасности и ответственности.
- **Центр по безопасному и ответственному использованию интернета** (**Center for Safe and Responsible Internet Use**, http://csriu.org) – Организация, обеспечивающая службы по работе с населением по вопросам безопасного и ответственного использования интернета.
- **Childnet International** (http://www.childnet-int.org) – Некоммерческая организация, которая вместе с партнерами по всему миру работает над тем, чтобы сделать интернет безопасным для детей.
- **ECPAT International** (http://www.ecpat.net) – Сеть организаций и частных лиц, работающих вместе для того чтобы уничтожить коммерческую сексуальную эксплуатацию детей.
- **GetNetWise** (http://www.getnetwise.org) – Служба общего пользования, обеспечиваемая коалицией корпораций интернет-отрасли и заинтересованными общественными организациями, которая стремится обеспечить для пользователей связь по "одному щелчку" с ресурсами, которые необходимы им для принятия обоснованных решений относительно индивидуального и семейного использования интернета.
- **Глобальный инфраструктурный альянс за безопасность интернета** (**Global Infrastructure Alliance for Internet Safety** (**GIAIS**), http://www.microsoft.com/security/msra/default.mspx) – Альянс поставщиков услуг интернета, которые объединились в целях укрепления защищенности и безопасности сети, согласованному отражению угроз широкого спектра и выявления и преодоления существующих уязвимостей.
- **INHOPE** (http://inhope.org) – Международная ассоциация, осуществляющая поддержку горячих линий интернета в части реагирования на сообщения о нелегальном контенте в целях повышения уровня безопасности интернета.
- **Internet Safety Group** (www.netsafe.org.nz) – Веб-сайт NetSafe – онлайновая база Группы по защите интернета Новой Зеландии (ISG) и Гектора защитника.
- **Международный центр помощи пропавшим и эксплуатируемым детям** (**International Centre for Missing & Exploited Children**, http://www.icmec.org) – Всемирное агентство, содействующее безопасности и благополучию детей посредством массовой политической активности, выработки политики и многонациональной координации.

- **Интерпол** (http://www.interpol.int) – Международная организация уголовной полиции, которая способствует международному сотрудничеству полицейских сил и оказывает поддержку и помощь всем организациям, органам и службам, целями которых являются предупреждение преступности и борьба с преступностью.
- **iSafe** (http://www.isafe.org) – Мировой лидер в области обучения по вопросам безопасности интернета; сочетает учебные программы в аудиториях и активную работу с населением, с тем чтобы предоставить возможность студентам, преподавателям, родителям, органам правопорядка и всем заинтересованным взрослым людям сделать интернет безопасным.
- **Microsoft Security At Home** (http://www.microsoft.com/protect) – Информация и ресурсы в помощь населению при обеспечении защиты своих компьютеров, собственной защиты и защиты своей семьи.
- **Национальный совет по материнству и детству** (**National Council for Motherhood and Childhood**, http://www.nccm.org.eg) – Египетская организация, призванная оказывать поддержку детству и материнству, используя подход, базирующийся на соблюдении прав.
- **Net Family News** (http://netfamilynews.org) – Некоммерческая общественная служба, организующая форум "новое в технологиях для детей" ("kid-tech news") для родителей и преподавателей из более чем 50 стран.
- **NetAlert Limited** (http://www.netalert.gov.au) – Некоммерческая общинная организация, учрежденная правительством Австралии для предоставления независимых консультаций и обучения в области доступа к онлайновому контенту.
- **NetSmartzKids** (http://www.netsmartzkids.org) – NetSmartz – это интерактивный образовательный ресурс по безопасности, организованный Национальным центром помощи пропавшим и эксплуатируемым детям (NCMEC) и Ассоциацией клубов для девочек и мальчиков Америки (BGCA), предназначенный для детей и подростков в возрасте от 5 до 17 лет, родителей, опекунов, преподавателей и правоохранительных органов и включающий соответствующие возрасту трехмерные программы для обучения детей безопасному поведению в интернете.
- "**За безопасность детей во всем мире**" (**Safe Kids Worldwide**, http://www.safekids.org) – Глобальная сеть организаций, имеющих целью предупреждение причинения случайного вреда подросткам, который является основной причиной смертности детей в возрасте до 14 лет.
- **SafeKids.com** (http://www.safekids.com) – Ресурсы в помощь семье, для того чтобы сделать пользование интернетом и технологиями привлекательным, безопасным и эффективным.
- **StaySafe.org** (http://www.staysafe.org) – Образовательный сайт, целью которого является помощь потребителям в понимании положительных аспектов интернета, а также способов решения различных вопросов защиты и безопасности, существующих в онлайновой среде.
- **ЮНИСЕФ** (http://www.unicef.org) – Глобальная организация по защите и поддержке прав детей, целью которой является предоставление долговременной гуманитарной помощи и помощи в области развитии детям и родителям в развивающихся странах.
- **WebSafe Crackerz** (http://www.websafecrackerz.com) – Интерактивные игры и головоломки, разработанные в помощь подросткам и предлагающие стратегии по разрешению различных ситуаций в онлайновой среде, включая спам, фишинг и различные виды мошенничества.

I.2 Пример списка адресов для оповещения об инцидентах

В таблице I.1, ниже, представлен пример перечня адресов для оповещения о случаях нарушения безопасности и защиты интернета:

Таблица I.1 – Примерный перечень контактной информации для оповещения о случаях нарушении безопасности

Организация	Адрес для контактов
Cisco Systems Inc.	mailto:safetyandsecurity@cisco.com http://www.cisco.com/security
Форум Группы реагирования на нарушения информационной безопасности (FIRST)	http://www.first.org/about/organization/teams/
Microsoft Corporation	mailto:avsubmit@submit.microsoft.com mailto:secure@microsoft.com
Telecom-ISAC Japan	https://www.telecom-isac.jp/contact/index.html

Библиография

[b-ITU-T X.1051] Рекомендация МСЭ-Т X.1051 (2004 г.), *Система управления информационной безопасностью – Требования к электросвязи (ISMS-T)*.

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information Technology – Security techniques – Information Security Management Systems – Requirements.*
http://www.iso.org/iso/catalogue-detail?csnumber=42103

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2009 г.