Приказ Минкомсвязи России от 25.08.2009 № 104 "Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования"

Зарегистрировано в Минюсте России 25.09.2009 № 14874

В целях реализации пункта 2 Постановления Правительства Российской Федерации от 18 мая 2009 г. № 424 "Об особенностях подключения федеральных государственных систем к информационно-телекоммуникационным сетям" (Собрание законодательства Российской Федерации, 2009, № 21, ст. 2573) приказываю:

1. Утвердить прилагаемые Требования по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования.

2. Направить настоящий Приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

3. Контроль за исполнением настоящего Приказа возложить на заместителя Министра связи и массовых коммуникаций Российской Федерации А.А. Солдатова.

Министр
И.О.Щеголев

Требования по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования

Утверждены
Приказом Министерства связи
и массовых коммуникаций
Российской Федерации
от 25.08.2009 № 104

1. Настоящие требования распространяются на федеральные государственные информационные системы, созданные или используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения, указанные в перечне сведений о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательных для размещения в информационно-телекоммуникационной сети «Интернет», утвержденном Постановлением Правительства Российской Федерации от 12 февраля 2003 г. № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» (Собрание законодательства Российской Федерации, 2003, № 7, ст. 658; 2008, № 48, ст. 5627) (далее - информационные системы общего пользования).

2. Организационно-техническое обеспечение устойчивого и безопасного функционирования информационных систем общего пользования представляет собой совокупность мероприятий, направленных на поддержание:
1) целостности информационной системы общего пользования как способности взаимодействия входящих в ее состав компонентов, при которой становится возможным выполнение функций по обработке информации;
2) устойчивости функционирования информационной системы общего пользования как ее способности сохранять свою целостность при отказе части компонентов системы, а также в условиях внутренних и внешних деструктивных информационных воздействий и возвращаться в исходное состояние;
3) безопасности информационной системы общего пользования как ее способности противостоять попыткам несанкционированного доступа к техническим и программным средствам системы и преднамеренным дестабилизирующим внутренним или внешним информационным воздействиям, следствием которых может быть нарушение ее функционирования.

3. Целостность информационной системы общего пользования обеспечивается совместимостью протоколов взаимодействия (функциональной совместимостью) и совместимостью интерфейсов технических средств (физической совместимостью) информационной системы общего пользования. Функциональная и физическая совместимость технических и программных средств информационной системы общего пользования обеспечивается выполнением требований, устанавливаемых в технической и эксплуатационной документации на систему.

4. Устойчивость функционирования информационной системы общего пользования обеспечивается:
1) разработкой мер при проектировании информационной системы общего пользования, направленных на выполнение требований к показателям надежности этой информационной системы общего пользования;
2) соблюдением условий эксплуатации, установленных в технической и эксплуатационной документации соответствующих технических и программных средств информационной системы общего пользования;
3) выполнением требований к информационной системе общего пользования в части технического обслуживания ее технических и программных средств;
4) выполнением требований к управлению информационной системой общего пользования в части контроля функционирования и анализа технических неисправностей в информационной системе общего пользования.

5. Показателем устойчивости функционирования информационной системы общего пользования является коэффициент

готовности, который определяется как вероятность того, что система окажется в работоспособном состоянии в произвольный момент времени ее функционирования (за исключением времени, в течение которого применение системы по назначению не предусматривается).

При выявлении несоответствия эксплуатационного значения коэффициента готовности технической норме должны проводиться мероприятия, направленные на определение причин выявленного несоответствия, и их устранение.

6. Безопасность информационной системы общего пользования обеспечивается разработкой мер при ее проектировании и эксплуатации, направленных на выполнение требований к безопасности этой информационной системы общего пользования.

7. В информационной системе общего пользования предусматривается подсистема безопасности, для которой:
1) основным назначением является обеспечение режима функционирования информационной системы общего пользования, при котором сохраняется целостность и доступность информации, содержащейся в информационной системе общего пользования;
2) разрабатывается Задание по безопасности, являющееся составной частью технического задания на разработку информационной системы общего пользования, которое включает в себя:
архитектуру построения и принципы взаимодействия подсистем, входящих в информационную систему общего пользования;
описание возможных нарушений целостности, устойчивости функционирования и безопасности информационной системы общего пользования;
описание подсистемы безопасности, включая систему защиты информации и систему антивирусной защиты программных средств (в том числе описание целевых функций, механизмов и используемых средств защиты, а также перечень защищаемых компонентов);
непротиворечивую политику безопасности (в том числе правила разграничения доступа, инструкции для оператора информационной системы общего пользования, а также порядок действий в нештатной ситуации).

8. В информационной системе общего пользования:
1) используются средства межсетевого экранирования, сертифицированные Федеральной службой по техническому и экспортному контролю;
2) используются системы обеспечения гарантированного электропитания (источники бесперебойного питания);
3) обеспечивается резервирование технических и программных средств.

9. В зависимости от значимости информационные системы общего пользования разделяются на два класса.

9.1. К классу I относятся информационные системы общего пользования: Правительства Российской Федерации, федеральных министерств, федеральных служб и федеральных агентств, руководство деятельностью которых осуществляет Президент Российской Федерации, федеральных служб и федеральных агентств, подведомственных этим федеральным министерствам.

9.2. К классу II относятся информационные системы общего пользования федеральных органов исполнительной власти, за исключением перечисленных в подпункте 9.1.

10. При создании и эксплуатации информационной системы общего пользования класса I:
1) используются сертифицированные Федеральной службой безопасности Российской Федерации антивирусные средства и средства обнаружения иного вредоносного программного обеспечения в соответствии с порядком, определенным Федеральной службой безопасности Российской Федерации;
2) обеспечивается защита от воздействий на технические и программные средства, в результате которых нарушается их функционирование, и защита от несанкционированного доступа к помещениям, в которых размещены данные средства, с использованием технических средств охраны, предотвращающих или существенно затрудняющих проникновение в помещения посторонних лиц, при этом помещения оборудованы охранной системой видеонаблюдения;
3) осуществляется регистрация действий обслуживающего персонала и аномальной активности пользователей;
4) расчетное значение коэффициента готовности, определяемое при проектировании, и эксплуатационное (оценочное) значение коэффициента готовности составляют не менее 0,99.

11. При создании и эксплуатации информационной системы общего пользования класса II:
1) используются сертифицированные Федеральной службой безопасности Российской Федерации антивирусные средства и средства обнаружения иного вредоносного программного обеспечения в соответствии с порядком, определенным их производителем;
2) обеспечивается защита от воздействий на технические и программные средства, в результате которых нарушается их функционирование, и защита от несанкционированного доступа к помещениям, в которых размещены данные средства;
3) осуществляется регистрация действий обслуживающего персонала;
4) расчетное значение коэффициента готовности, определяемое при проектировании, и эксплуатационное (оценочное) значение коэффициента готовности составляют не менее 0,95.

12. Операторы информационной системы общего пользования обязаны обеспечивать:
1) недопущение воздействия на технические и программные средства информационной системы общего пользования, в результате которого нарушается их функционирование;
2) предупреждение возможных неблагоприятных последствий нарушения порядка доступа к техническим и программным средствам информационной системы общего пользования;
3) постоянный контроль обеспечения защищенности информационной системы общего пользования от неправомерных действий.

техническая защита информации

From:
http://www.sps-ib.ru/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
http://www.sps-ib.ru/npa:minkomsvyaz104_25.08.2009

Last update: **2016/09/09 09:16**