Приказ ФСБ России № 416, ФСТЭК России № 489 от 31.08.2010 "Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования"

Зарегистрировано в Минюсте России 13 октября 2010 г. № 18704

В соответствии с пунктом 3 Постановления Правительства Российской Федерации от 18 мая 2009 г. № 424[1)] приказываем:

1. Утвердить прилагаемые Требования о защите информации, содержащейся в информационных системах общего пользования.

2. Контроль за исполнением настоящего Приказа возложить на руководителя Научно-технической службы Федеральной службы безопасности Российской Федерации и первого заместителя директора Федеральной службы по техническому и экспортному контролю.

Директор
Федеральной службы безопасности
Российской Федерации
А.Бортников

Директор
Федеральной службы
по техническому
и экспортному контролю
С.Григоров

Требования о защите информации, содержащейся в информационных системах общего пользования

Приложение
к Приказу ФСБ России, ФСТЭК России
от 31 августа 2010 г. № 416/489

1. Настоящие Требования распространяются на федеральные государственные информационные системы, созданные или используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательные для размещения в информационно-телекоммуникационной сети Интернет, определяемые Правительством Российской Федерации[2)] (далее - информационные системы общего пользования), и являются обязательными для операторов информационных систем общего пользования при разработке и эксплуатации информационных систем общего пользования.

2. Информационные системы общего пользования должны обеспечивать:
сохранность и неизменность обрабатываемой информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения (далее - целостность информации);
беспрепятственный доступ пользователей к содержащейся в информационной системе общего пользования информации (далее - доступность информации);
защиту от действий пользователей в отношении информации, не предусмотренных правилами пользования информационной системой общего пользования, приводящих в том числе к уничтожению, модификации и блокированию информации (далее - неправомерные действия).

3. Информационные системы общего пользования включают в себя средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

4. Информация, содержащаяся в информационной системе общего пользования, является общедоступной.

5. Информационные системы общего пользования в зависимости от значимости содержащейся в них информации и требований к ее защите разделяются на два класса.

5.1. К I классу относятся информационные системы общего пользования Правительства Российской Федерации и иные информационные системы общего пользования в случае, если нарушение целостности и доступности информации, содержащейся в них, может привести к возникновению угроз безопасности Российской Федерации. Отнесение информационных систем общего пользования к I классу проводится по решению руководителя соответствующего федерального органа исполнительной власти.

5.2. Ко II классу относятся информационные системы общего пользования, не указанные в подпункте 5.1 настоящего пункта.

6. Защита информации, содержащейся в информационных системах общего пользования, достигается путем исключения неправомерных действий в отношении указанной информации.

7. Методы и способы защиты информации в информационных системах общего пользования определяются оператором информационной системы общего пользования и должны соответствовать настоящим Требованиям.

Достаточность принятых мер по защите информации в информационных системах общего пользования оценивается при проведении мероприятий по созданию данных систем, а также в ходе мероприятий по контролю за их функционированием.

8. Работы по защите информации в информационных системах общего пользования являются неотъемлемой частью работ по созданию данных систем.

9. Размещение информационных систем общего пользования, специальное оборудование и охрана помещений, в которых находятся технические средства, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей информации и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

10. Защиту информации в информационных системах общего пользования обеспечивает оператор информационной системы общего пользования.

11. В информационных системах общего пользования должны быть обеспечены:
поддержание целостности и доступности информации;
предупреждение возможных неблагоприятных последствий нарушения порядка доступа к информации;
проведение мероприятий, направленных на предотвращение неправомерных действий в отношении информации;
своевременное обнаружение фактов неправомерных действий в отношении информации;
недопущение воздействия на технические средства информационной системы общего пользования, в результате которого может быть нарушено их функционирование;
возможность оперативного восстановления информации, модифицированной или уничтоженной вследствие неправомерных действий;
проведение мероприятий по постоянному контролю за обеспечением их защищенности;
возможность записи и хранения сетевого трафика.

12. Мероприятия по обеспечению защиты информации в информационных системах общего пользования включают в себя:
определение угроз безопасности информации, формирование на их основе модели угроз;
разработку на основе модели угроз системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты информации, предусмотренных для соответствующего класса информационных систем общего пользования;
проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
обучение лиц, использующих средства защиты информации, применяемые в информационной системе общего пользования, правилам работы с ними;
учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
проведение разбирательств и составление заключений по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению безопасности информации или другим нарушениям, снижающим уровень защищенности информационной системы общего пользования, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
описание системы их защиты.

13. Для разработки и осуществления мероприятий по защите информации в информационных системах общего пользования оператором информационной системы общего пользования назначается структурное подразделение или должностное лицо (работник), ответственные за обеспечение защиты информации.

14. Запросы пользователей на получение информации, содержащейся в информационных системах общего пользования, а также факты предоставления информации по этим запросам регистрируются автоматизированными средствами информационных систем общего пользования в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора информационной системы общего пользования.

15. При обнаружении нарушений порядка доступа к информации оператор информационной системы общего пользования организует работы по выявлению причин нарушений и устранению этих причин в установленном порядке. Подсистема информационной безопасности должна обеспечивать восстановление информации в информационной системе общего пользования, модифицированной или уничтоженной вследствие неправомерных действий в отношении такой информации. Время восстановления процесса предоставления информации пользователям не должно превышать 8 часов.

16. Реализация требований по обеспечению защиты информации в средствах защиты информации возлагается на их разработчиков.

17. При создании и эксплуатации информационных систем общего пользования должны выполняться следующие требования по защите информации:

17.1. В информационных системах общего пользования I класса:

использование средств защиты информации от неправомерных действий, в том числе средств криптографической защиты информации (электронной цифровой подписи, при этом средства электронной цифровой подписи обязательно должны применяться к публикуемому информационному наполнению), сертифицированных ФСБ России;
использование средств обнаружения вредоносного программного обеспечения, в том числе антивирусных средств, сертифицированных ФСБ России;
использование средств контроля доступа к информации, в том числе средств обнаружения компьютерных атак, сертифицированных ФСБ России;
использование средств фильтрации и блокирования сетевого трафика, в том числе средств межсетевого экранирования, сертифицированных ФСБ России;
осуществление локализации и ликвидации неблагоприятных последствий нарушения порядка доступа к информации;
осуществление записи и хранения сетевого трафика при обращении к государственным информационным ресурсам за десять и более последних дней и предоставление доступа к записям по запросам уполномоченных государственных органов, осуществляющих оперативно-разыскную деятельность;
обеспечение защиты от воздействий на технические и программные средства информационных систем общего пользования, в результате которых нарушается их функционирование, и несанкционированного доступа к помещениям, в которых находятся данные средства, с использованием технических средств охраны, в том числе систем видеонаблюдения, предотвращающих проникновение в помещения посторонних лиц;
осуществление регистрации действий обслуживающего персонала и пользователей;
обеспечение резервирования технических и программных средств, дублирования носителей и массивов информации;
использование сертифицированных в установленном порядке систем обеспечения гарантированного электропитания (источников бесперебойного питания);
осуществление мониторинга их защищенности уполномоченным подразделением ФСБ России;
введение в эксплуатацию только после направления оператором информационной системы общего пользования в ФСБ России уведомления о готовности ввода информационной системы общего пользования в эксплуатацию и ее соответствии настоящим Требованиям.

17.2. В информационных системах общего пользования II класса:
использование средств защиты информации от неправомерных действий, сертифицированных ФСБ России и (или) ФСТЭК России с учетом их компетенции, в том числе средств криптографической защиты информации (электронной цифровой подписи, при этом средства электронной цифровой подписи должны применяться к публикуемому информационному наполнению);
использование средств обнаружения вредоносного программного обеспечения, в том числе антивирусных средств, сертифицированных ФСБ России и (или) ФСТЭК России с учетом их компетенции;
использование средств контроля доступа к информации, в том числе средств обнаружения компьютерных атак, сертифицированных ФСБ России и (или) ФСТЭК России с учетом их компетенции;
использование средств фильтрации и блокирования сетевого трафика, в том числе средств межсетевого экранирования, сертифицированных ФСБ России и (или) ФСТЭК России с учетом их компетенции;
осуществление локализации и ликвидации неблагоприятных последствий нарушения порядка доступа к информации;
осуществление записи и хранения сетевого трафика при обращении к государственным информационным ресурсам за последние сутки и более и предоставление доступа к записям по запросам уполномоченных государственных органов, осуществляющих оперативно-разыскную деятельность;
обеспечение защиты от воздействий на технические и программные средства информационных систем общего пользования, в результате которых нарушается их функционирование, и несанкционированного доступа к помещениям, в которых находятся данные средства;
осуществление регистрации действий обслуживающего персонала;
обеспечение частичного резервирования технических средств и дублирования массивов информации;
использование систем обеспечения гарантированного электропитания (источников бесперебойного питания);
осуществление мониторинга их защищенности уполномоченным подразделением ФСБ России;
введение в эксплуатацию только после направления оператором информационной системы общего пользования в ФСТЭК России уведомления о готовности ввода информационной системы общего пользования в эксплуатацию и ее соответствии настоящим Требованиям.

техническая защита информации

[1)] Собрание законодательства Российской Федерации, 2009, № 21, ст. 2573.

[2)] Постановление Правительства Российской Федерации от 24 ноября 2009 г. № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» (Собрание законодательства Российской Федерации, 2009, № 48, ст. 5832).

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

Permanent link:
http://www.sps-ib.ru/npa:416-489_31.08.2010

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