Об утверждении Инструкции по проведению проверок состояния защищенности информационных сетей и ресурсов государственных органов и организаций Республики Казахстан

Приказ Руководителя Канцелярии Премьер-Министра Республики Казахстан от 21 мая 2012 года № 25-1-50. Зарегистрирован в Министерстве юстиции Республики Казахстан 18 июня 2012 года № 7740.

В соответствии с подпунктом 21) пункта 12 Положения о Канцелярии Премьер-Министра Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 11 сентября 2002 года № 993, **ПРИКАЗЫВАЮ**:

1. Утвердить прилагаемую Инструкцию по проведению проверок состояния защищенности информационных сетей и ресурсов государственных органов и организаций Республики Казахстан.

2. Отделу по защите государственных секретов Канцелярии Премьер-Министра Республики Казахстан (Толымбеков М.И.) в установленном законодательством порядке обеспечить государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан.

3. Контроль за исполнением настоящего приказа возложить на заведующего Отделом по защите государственных секретов Канцелярии Премьер-Министра Республики Казахстан Толымбекова М.И.

4. Настоящий приказ вводится в действие со дня государственной регистрации в Министерстве юстиции Республики Казахстан.

Руководитель Канцелярии Е. Кошанов

СОГЛАСОВАНО
Генеральный прокурор
Республики Казахстан
_____ А. Даулбаев
14 мая 2012 года

СОГЛАСОВАНО
Министр финансов
Республики Казахстан
_____ Б. Жамишев
15 мая 2012 года

СОГЛАСОВАНО
Председатель Комитета
национальной безопасности
Республики Казахстан
_____ Н. Абыкаев
14 мая 2012 года

СОГЛАСОВАНО
Министр транспорта и
коммуникации
Республики Казахстан
_____ А. Жумагалиев
15 мая 2012 года

Утверждена
приказом Руководителя
Канцелярии Премьер-Министра
Республики Казахстан
от 21 мая 2012 года № 25-1-50

Инструкция
по проведению проверок состояния защищенности информационных сетей и ресурсов государственных органов и организаций Республики Казахстан

Настоящая Инструкция по проведению проверок состояния защищенности информационных сетей и ресурсов государственных органов и организаций Республики Казахстан (далее - Инструкция) разработана в соответствии с законами Республики Казахстан "О государственном контроле и надзоре в Республике Казахстан " от 6 января 2011 года, "Об информатизации" от 11 января 2007 года, "О техническом регулировании" от 9 ноября 2004 года, Правилами проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам, утвержденных постановлением Правительства Республики Казахстан от 30 декабря 2009 года № 2280 (далее – постановление), СТ РК ИСО/МЭК 17799-2006 "Методы обеспечения защиты. Свод правил по управлению защитой информации", ГОСТ РК ИСО/МЭК 27001-2006 " Информационные технологии. Методы и средства обеспечения безопасности. Системы

менеджмента информационной безопасности. Требования", СТ РК ГОСТ Р 50739-2006 "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования", СТ РК 34.022-2006 "Защита информации. Требования к проектированию, установке, наладке, эксплуатации и обеспечению безопасности информационных систем" и определяют порядок проведения проверок состояния информационной безопасности в государственных органах и организациях, за исключением проверок информационных систем в защищенном исполнении*.

1. Общие положения

1. Проверка состояния защищенности информационных сетей и ресурсов государственных органов и организаций (далее - проверка) осуществляется уполномоченным государственным органом по защите государственных секретов и обеспечению информационной безопасности (далее - уполномоченный орган) с привлечением соответствующих специалистов органов национальной безопасности, уполномоченного государственного органа в области информатизации, уполномоченной организации в области информатизации и соответствующих подразделений по защите государственных секретов, проверяемых государственных органов и организаций. Для проведения проверки уполномоченным органом формируется состав проверочной комиссии (далее – Комиссия), указываемый в предписании уполномоченного органа на проведение проверки.

2. Проверки состояния защищенности информационных сетей и ресурсов государственных органов и организаций осуществляются с целью определения соответствия нормативных, организационных, практических и технических мероприятий, реализуемых государственными органами и организациями, требованиям нормативных правовых актов и стандартов Республики Казахстан в области информационной безопасности, защиты информации.

3. Проверка осуществляется на основании предписания уполномоченного органа, подписанного первым руководителем и заверенного гербовой печатью, с предъявлением проверяющими документов, удостоверяющих личность. Предписание готовится в 2-х экземплярах, первый экземпляр которого остается в проверяемой организации.

4. Уполномоченный орган письменно уведомляет организацию о предстоящей проверке за 10 календарных дней до ее начала.

2. Проведение проверки

5. Проверка состояния защищенности информационных сетей и ресурсов государственных органов и организаций включает:

1) определение установленных на объекте технологических режимов обработки информации, используемых информационных систем, характера циркулирующей информации в информационных системах;

2) наличие организационно-распорядительной документации, учитывающей конкретные условия функционирования средств вычислительной техники различного уровня и назначения (рабочие станции пользователей, серверное и иное периферийное оборудование, технические средства защиты информации, в том числе средства криптографической защиты информации, кроме государственных шифровальных средств), порядок работы сотрудников организации при эксплуатации средств вычислительной техники (в соответствии с постановлением):

приказ руководителя организации, регламентирующий порядок организации обеспечения информационной безопасности;

политика информационной безопасности организации;

Правила паспортизации средств вычислительной техники и использования информационных ресурсов корпоративной сети;

Инструкция о парольной защите;

Инструкция о порядке действий пользователей во внештатных (кризисных) ситуациях;

Инструкция по организации антивирусной защиты;

Инструкция пользователя по эксплуатации и обслуживанию компьютерного оборудования и программного обеспечения;

Инструкция о резервном копировании информации;

Правила регистрации пользователей в корпоративной информационной сети организации;

Памятка для работы системных администраторов;

Памятка пользователей средств вычислительной техники;

3) определение круга технических специалистов, имеющих доступ к средствам вычислительной техники, информационных систем и базам данных, проверка функционально закрепленных обязанностей сотрудников организации;

4) организация и фактическое состояние работ по защите информации при проведении технического обслуживания, ремонта и других работ средств вычислительной техники, информационных систем и баз данных с привлечением сторонних организаций;

5) анализ принятых мер (программных, технических, организационных), обеспечивающих защиту средств вычислительной техники, информационных систем и баз данных от несанкционированного доступа. Оценка продуктивности организационного процесса защиты информации. Достаточность технических средств обработки и защиты информации, наличие подтверждений соответствия по требованиям информационной безопасности (сертификатов);

6) проведение анализа конфигураций активного сетевого оборудования, маршрутизаторов, коммутаторов, серверов с целью выявления уязвимых мест в системе защиты информации;

7) проведение инструментального анализа сетевого и серверного оборудования локально-вычислительных сетей, информационных систем и баз данных с применением программно-аппаратных средств;

8) проверка работоспособности используемых программно-аппаратных средств обнаружения и предотвращения компьютерных атак;

9) проверка наличия лицензионных средств защиты от вредоносных программ и вирусов или сертифицированных свободно распространяемых антивирусных средств защиты;

10) организация работы по обеспечению доступа сотрудников организации к глобальной информационной сети Интернет, анализ защищенности средств вычислительной техники от несанкционированного доступа из сети Интернет;

11) проверка оснащения серверных и кроссовых помещений средствами контроля доступа и пожаротушения, обеспечения температурного режима, регламент доступа к серверным и кроссовым помещениям;

12) состояние защищенности информационных ресурсов от сбоев в системе электропитания (схема резервирования, система автоматического ввода резерва);

13) состояние линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

6. Проверяемая организация обеспечивает предоставление своими работниками объяснений (устно и письменно) на вопросы проверяющих, доступ к информации, в том числе к автоматизированным системам. Предоставляет возможность членам комиссии снятия копий необходимых документов, а также оказывает комиссии содействие в своевременном проведении и завершении проверки.

7. Члены Комиссии при проведении проверки обеспечивают сохранность полученных от организации документов и конфиденциальность содержащейся в них информации.

8. Работа Комиссии (проверяющего) завершается подведением итогов (обобщением) результатов проверки и составлением акта в произвольной форме.

9. Акт должен содержать:

1) дата, время и место составления акта;

2) наименование органа контроля и надзора;

3) дата и номер акта о назначении проверки, на основании которого проведена проверка;

4) фамилия, имя, отчество (при его наличии) и должность лица (лиц), проводившего проверку;

5) наименование или фамилия, имя, отчество (при его наличии) проверяемого субъекта, должность представителя физического или юридического лица, присутствовавших при проведении проверки;

6) дата, место и период проведения проверки;

7) сведения о результатах проверки, в том числе о выявленных нарушениях, об их характере;

8) сведения об ознакомлении или об отказе в ознакомлении с актом представителя проверяемого субъекта, а также лиц, присутствовавших при проведении проверки, их подписи или отказ от подписи;

9) подпись должностного лица (лиц), проводившего проверку;

10) достоверное и обоснованное изложение состояния защищенности информационных сетей и ресурсов организации, выявленных недостатков и нарушений со ссылками на соответствующие документы и факты, выводы и предложения по их устранению с указанием конкретных сроков;

11) объективно отражать практическую деятельность подразделения по информатизации, ответственного за обеспечение информационной безопасности, и руководства организации по обеспечению защиты информационных сетей и ресурсов.

Акт составляется в двух экземплярах. Первый для проверяемой организации, а второй - для уполномоченного органа.

10. С актом знакомятся руководители организации, а при необходимости и отдельные исполнители, в части их касающейся, которые подписывают его или прилагают к нему свои письменные объяснения с замечаниями и возражениями.

11. Об устранении выявленных в результате проверки недостатков и нарушений и реализации предложений руководитель проверяемой организации в установленные в акте сроки сообщает в уполномоченный орган и, в установленных (необходимых) случаях, в вышестоящую организацию.