Об утверждении Правил проведения аудита информационных систем

Утративший силу

Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 134. Зарегистрирован в Министерстве юстиции Республики Казахстан 25 февраля 2016 года № 13258. Утратил силу приказом Министра информации и коммуникаций Республики Казахстан от 13 июня 2018 года № 263 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования)

Сноска. Утратил силу приказом Министра информации и коммуникаций РК от 13.06.2018 № 263 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В соответствии с подпунктом 22) статьи 7 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" **ПРИКАЗЫВАЮ:**

1. Утвердить прилагаемые Правила проведения аудита информационных систем.

2. Признать утратившим силу приказ Министра связи и информации Республики Казахстан от 20 августа 2010 года № 200 "Об утверждении Правил проведения аудита информационных систем" (зарегистрированный в Реестре государственной регистрации нормативных правовых актов Республики Казахстан под № 6488, опубликованный 6 ноября 2010 года в газете " Казахстанская правда" и 9 ноября 2010 года в газете "Егемен Қазақстан").

3. Комитету связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан (Қазанғап Т.Б.) обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) направление копии настоящего приказа в печатном и электронном виде на официальное опубликование в периодические печатные издания и информационно-правовую систему "Әділет" в течение десяти календарных дней после его государственной регистрации в Министерстве юстиции Республики Казахстан, а также в Республиканский центр правовой информации в течение десяти календарных дней со дня получения зарегистрированного приказа для включения в эталонный контрольный банк нормативных правовых актов Республики Казахстан;

3) размещение настоящего приказа на интернет-ресурсе Министерства по инвестициям и развитию Республики Казахстан и на интранет-портале государственных органов;

4) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства по инвестициям и развитию Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1), 2) и 3) пункта 3 настоящего приказа.

4. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра по инвестициям и развитию Республики Казахстан.

5. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Исполняющий обязанности
Министра по инвестициям и развитию,
Республики Казахстан Ж. Касымбек

Утверждены
приказом исполняющего
обязанности Министра
по инвестициям и развитию
Республики Казахстан
от 28 января 2016 года № 134

Правила проведения аудита информационных систем

1. Общие положения

1. Настоящие Правила проведения аудита информационных систем (далее - Правила) разработаны в соответствии с подпунктом 22) статьи 7 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" (далее - Закон) и определяют порядок проведения аудита как информационных систем государственных органов, так и негосударственных информационных систем.

2. Аудит информационных систем осуществляется с целью получения оценки текущего состояния информационных систем, действий и событий, происходящих в них, определяющих уровень их соответствия техническим регламентам, стандартам в сфере информатизации, нормативно-технической документации и (или) требованиям заказчика, а также требованиям информационной безопасности.

3. В настоящих правилах используются следующие понятия:

1) аудит информационной системы – независимое обследование информационной системы в целях повышения эффективности ее использования;

2) информационно-коммуникационная инфраструктура – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

3) уполномоченный орган в сфере информатизации (далее - уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию в сфере информатизации и "электронного правительства";

4) нормативно-техническая документация – совокупность документов, определяющих общие задачи, принципы и требования к созданию и использованию (эксплуатации) объектов информатизации, а также контролю их соответствия установленным требованиям в сфере информатизации.

4. Аудит информационных систем проводится на этапе создания, внедрения и эксплуатации информационных систем по инициативе собственника или владельца информационных систем.

5. Проведение аудита информационных систем осуществляется физическим и (или) юридическим лицами, обладающими специальными знаниями и опытом работы в области информационно-коммуникационных технологий.

6. Аудит информационных систем в защищенном исполнении, отнесенных к государственным секретам, не проводятся.

7. Заказчиком аудита информационных систем является собственник и (или) владелец информационной системы.

8. Основными направлениями аудита информационных систем являются оценка:

1) соответствия функций информационной системы его целям и задачам;

2) соответствия разработки, внедрения, сопровождения и эксплуатации информационной системы стандартам в сфере информатизации;

3) уровня защищенности информационных систем, включая прикладное программное обеспечение и базы данных;

4) состояния информационно-коммуникационной инфраструктуры ее технического состояния и топологии;

5) соответствия нормативно-технической документации стандартным требованиям;

6) соответствия требованиям информационной безопасности.

9. Аудит информационных систем проводится в соответствии с договором между заказчиком и лицом, обладающим специальными знаниями и опытом работы в сфере информационно-коммуникационных технологий.

10. При проведении аудита государственных информационных систем выбор лиц, обладающих специальными знаниями и опытом работы в области информационно-коммуникационных технологий, осуществляется в соответствии с главой 4 Закона Республики Казахстан от 4 декабря 2015 года "О государственных закупках", по итогам которого подписывается соответствующий договор о государственных закупках на проведение аудита информационных систем.

11. Расходы по проведению аудита информационных систем несет сторона, определенная по согласованному решению между собственником и (или) владельцем информационной системы.

12. Срок проведения аудита информационный системы зависит от функциональной сложности информационной системы, количества структурных компонентов (подпрограмм), условий ее эксплуатации (организация рабочих мест, доступ к серверам, наличия региональных (территориальных) центров сопровождения информационной системы), а также конкретных целей аудита информационный системы со стороны заказчика и указывается в договоре.

13. По результатам аудита информационный системы готовится аудиторское заключение по результатам проведения аудита информационной системы (далее – заключение) по форме, согласно приложению к настоящим Правилам.

14. Заключение заверяется подписями лиц осуществляющих аудит информационных систем и заказчика, скрепляется печатью лиц осуществляющих аудит информационных систем.

15. Заключение составляется на государственном и русском языках в 2 (двух) экземплярах, один из которых передается заказчику, второй остается у организации.

16. Копия заключения по информационным системам государственных органов, и негосударственным информационным системам, интегрируемых с информационными системами государственных органов заказчик передает уполномоченному органу в сфере информатизации.

17. Заключение носит рекомендательный характер.

2. Порядок проведения аудита информационных систем

18. Назначением и основными целями аудита информационных систем являются:

1) получение объективной и независимой оценки текущего состояния защищенности информационных ресурсов;

2) получение максимальной отдачи от средств, инвестируемых в создание системы информационной безопасности;

3) оценка возможного ущерба от несанкционированных действий;

4) разработка требований к построению системы защиты информации;

5) определение зон ответственности сотрудников подразделений;

6) разработка порядка и последовательности внедрения системы информационной безопасности.

19. Задачами аудита информационных систем являются:

1) анализ и оценка разработки политик безопасности и других организационно-распорядительных документом по защите информационных систем;

2) анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационных систем;

3) оценка постановки задач для персонала, касающихся обеспечения защиты информации;

4) оценка участия в разборе инцидентов, связанных с нарушением информационной безопасности;

5) локализация уязвимых мест в системе защиты информационных систем;

6) определение степени участия в обучении пользователей и обслуживающего персонала информационных систем вопросам обеспечения информационной безопасности;

7) выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности информационных систем.

20. Работы по аудиту информационных систем включают в себя ряд последовательных этапов, которые в целом соответствуют этапам проведения аудита информационных систем, который включает в себя следующее:

1) инициирование процедуры аудита информационных систем;

2) сбор информации аудита информационных систем;

3) анализ данных аудита информационных систем;

4) выработка рекомендаций;

5) подготовка заключения.

21. К основным видам работ по аудиту информационных систем относятся:

1) проведение анализа экспертным методом;

2) оценка соответствия рекомендациям стандартов по информационной безопасности и единым требованиям в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утверждаемым в соответствии с подпунктом 3) статьи 6 Закона;

3) инструментальное обследование компонентов информационных систем.

22. В ходе проведения анализа экспертным методом выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в процедуре обследования.

23. В качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты используются стандарты СТ РК ИСО/МЭК 27001-2008 "Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования", СТ РК ИСО /МЭК 27002-2009 "Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информации" и СТ РК ГОСТ Р 50739-2006 " Средства вычислительной техники Защита от несанкционированного доступа к информации Общие технические требования".

24. По стандартам СТ РК ИСО/МЭК 27001-2008 "Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования", СТ РК ИСО/МЭК 27002-2009 " Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информации" к основным ключевым критериям аудита информационных систем относятся следующие разделы:

1) политика безопасности;
2) организация защиты;
3) классификация ресурсов и их контроль;
4) безопасность персонала;
5) физическая безопасность;
6) администрирование информационных систем и вычислительных сетей;
7) управление доступом;
8) разработка и сопровождение информационных систем;
9) планирование бесперебойной работы организации;
10) контроль выполнения требований политики безопасности.

25. По СТ РК ГОСТ Р 50739-2006 "Средства вычислительной техники Защита от несанкционированного доступа к информации Общие технические требования " к основным ключевым критериям аудита информационных систем относятся:

1) реализация основных требований к разграничению доступа (дискретизационный принцип контроля доступа);
2) реализация мандатного принципа контроля доступом;
3) реализация идентификации и аутентификации доступа пользователей;
4) показатель регистрация;
5) маркировка документов;
6) основные требования к гарантиям;
7) требования к документации.

26. При инструментальном обследовании компонентов информационных систем они направляются на выявление и устранение уязвимостей программно-аппаратного обеспечения системы.

27. Оформление результатов аудита информационных систем включает:

1) оценку соответствия стандартам СТ РК ИСО/МЭК 27001-2008 " Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования", СТ РК ИСО /МЭК 27002-2009 "Информационные технологии.

Средства обеспечения. Свод правил по управлению защитой информации" и СТ РК ГОСТ Р 50739-2006 "Средства вычислительной техники

Защита от несанкционированного доступа к информации

Общие технические требования";

2) результаты инструментального обследования;

3) выработку рекомендаций;

4) подготовку заключения.

Приложение
к Правилам проведения
аудита информационных систем

Форма

Аудиторское заключение
по результатам проведения аудита информационной системы

_____
___

(наименование информационной системы)

_____
___

(наименование организации заказчика)

в области _____ _____
_

(область проведения аудита)

от "___" _____ 20__ г.

_____
___

(наименование лица, осуществляющего аудит информационных систем)

согласно договору от "___" _____ 20__ г. проведен аудит в соответствии с Правилами проведения аудита информационных систем (отчет о проведении аудита информационных систем с организационными, техническими, методологическими аспектами проведенного аудита

прилагается).

В ходе аудиторской проверки было установлено, что данная информационная система имеет следующие оценочные показатели:

1. _____
2. _____
3. _____

что соответствует/не соответствует установленным требованиям и стандартам в области _____

(область проведения аудита)

Рекомендации по сопровождению и развитию информационной системы

_____

___

_____

___

"___" _____ 20__ г. _____

(ФИО, подпись)