# Аудит информационной безопасности объектов топливно-энергетического комплекса

*Лившиц И.И., д.т.н., профессор практики, Университет ИТМО*
*+7 (921) 934-48-46*
*Livshitz.il@yandex.ru*

## Аннотация

В представленной публикации кратко рассмотрены аспекты выполнения аудита информационной безопасности объектах топливно-энергетического комплекса на примере подземного хранилища газа. Приняты во внимание современные требования к обеспечению безопасности объектов топливно-энергетического комплекса, в том числе – Федеральные законы, актуальные международные ISO (ISO/IEC) и национальные стандарты ГОСТ Р.

Формулировка проблемы затрагивает способность достижения целей аудита информационной безопасности при известных ограничениях по срокам, ресурсам и территориальному охвату. Решение проблемы предполагается в рамках унификации общих концептуальных требования применимого национального законодательства и лучших практик в области стандартизации аудита систем менеджмента информационной безопасности. Полученные результаты могут найти применение при формировании собственных команд аудиторов и обеспечения заданного уровня безопасности на объектах топливно-энергетического комплекса РФ в современных условиях.

## Ключевые слова

Аудит, система менеджмента, объект, топливно-энергетический комплекс, подземное хранилище газа, федеральное законодательство, ГОСТ, ISO, ISO/IEC.

## Введение

В настоящее время следует признать высокую важность обеспечения безопасности объектов топливно-энергетического комплекса (далее – ТЭК). Актуальность данной проблемы сложно переоценить, поскольку приняты необходимые нормы Федерального законодательства, разработаны и применяются многочисленные национальные (система ГОСТ Р) и международные (ISO и ISO/IEC) стандарты, создана хорошая отраслевая практика. В то же время известны негативные инциденты: атаки в 2019 г. на нефтяные объекты Saudi Aramro в Саудовской Аравии[1] и атаки в 2017 г. на компьютеры «Башнефти»[2] вируса WannaCry в Башкирии. Следует отметить, что общий ущерб деятельности указанным крупнейшим объектам ТЭК косвенно вызван и нарушением нормального функционирования ИТ-инфраструктуры, соответственно, далее будет исследоваться проблема обеспечения информационной безопасности (далее – ИБ) и более конкретно – проблема эффективного аудита ИБ. В открытом доступе достаточно публикаций о том, как невнимание к вопросам аудита ИБ может привести к значительным финансовым и репутационным издержкам (на примере корпорации РЖД[3]).

На тему аудитов ИБ применительно к объектам ТЭК известны публикации ([1, 4]), в которых рассмотрены как общие вопросы аудита, так и конкретные методики выполнения аудитов в рамках интегрированных систем менеджмента далее – (ИСМ). Для целей данной публикации будет выбран конкретный объект – подземное хранилище газа (далее – ПХГ), для которого в рамках учебного процесса в Университете ИТМО была подготовлена реальная программа аудита ИБ и выполнена практическая отработка современных методик аудита ИБ в ИСМ. В качестве нормативно-методической базы применялись стандарты в области аудита ISO/IEC серии 19011 [5] и стандарты ISO/IEC семейства 27000 [6 – 11].

## Нормативная база аудита – Федеральное законодательство

В качестве нормативной базы аудита ИБ для ПХГ были рассмотрены Федеральный закон от 21 июля 2011 г. N 256-ФЗ "О безопасности объектов топливно-энергетического комплекса"[4]

[1] https://tass.ru/mezhdunarodnaya-panorama/6887707
[2] https://www.forbes.ru/kompanii/346997-rosneft-pozhalovalas-na-moshchnuyu-hakerskuyu-ataku
[3] https://habr.com/ru/news/t/526852/
[4] https://base.garant.ru/12188188

(далее – ФЗ-256) и Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"[5] (далее – ФЗ-187). Следует отметить, что при планировании аудитов в национальной юрисдикции всегда следует начинать с изучения применимого Федерального законодательства, далее уже следует применять соответствующие общие требования международных и национальных стандартов. Данный порядок рекомендуется по причине отсутствия в Федеральном законодательстве РФ требований к конкретным видам аудита (или оценки соответствия), в том числе, аудитов ИБ, применительно к конкретным объектам ТЭК. В частности и ФЗ-256 и ФЗ-187 не содержат по тексту упоминания терминов «аудит» и/или «оценка соответствия», но эти термины, безусловно, присутствуют в «целевых» стандартах по аудиту [5, 7, 11].

ФЗ-256 в Ст.3 устанавливает цели и задачи обеспечения безопасности объектов ТЭК, цитата: «*Целями обеспечения безопасности объектов топливно-энергетического комплекса являются их* ***устойчивое и безопасное функционирование****, защита интересов личности, общества и государства в сфере топливно-энергетического комплекса от актов незаконного вмешательства*». Следует заметить, что ФЗ-256 дает хорошее обоснование для документирования объектов ТЭК, в частности, в Ст.8 (2) установлены требования к паспорту безопасности объекта ТЭК: «*Паспорт безопасности объекта топливно-энергетического комплекса составляется на основании результатов категорирования данного объекта в зависимости от степени его потенциальной опасности, а также* ***на основании оценки достаточности*** *инженерно-технических мероприятий, мероприятий по физической защите и охране объекта при террористических угрозах согласно требованиям, определенным Правительством Российской Федерации в соответствии со статьей 7 настоящего Федерального закона».*

ФЗ-187 в Ст. 2 (2) вводит термин «безопасность критической информационной инфраструктуры»: «*состояние защищенности критической информационной инфраструктуры, обеспечивающее ее* ***устойчивое функционирование*** *при проведении в отношении ее компьютерных атак»*. В Ст. 2 (7) дается определение «объект критической информационной инфраструктуры»: «*информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры*»; а в Ст.2 (8) введено подробно описание субъекта критической информационной инфраструктуры, в том числе ТЭК.

Необходимо отметить, что Ст. 12 ФЗ-187 «Оценка безопасности критической информационной инфраструктуры» явно определяет, что оценка осуществляется, цитата: «*федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в целях прогнозирования возникновения возможных угроз безопасности критической информационной инфраструктуры и выработки мер по повышению устойчивости ее функционирования при проведении в отношении ее компьютерных атак».* Соответственно, из буквального толкования норм ФЗ-187 следует только обязанность осуществления оценки безопасности для объектов ТЭК, но не установлены ограничения на выполнение аудита ИБ, например, в соответствии с требованиями ГОСТ Р или ISO/IEC 27001 или в общем – при аудите ИСМ на объектах ТЭК.

## Нормативная база аудита – Национальные стандарты

В качестве нормативной базы аудита ИБ для ПХГ были рассмотрены два основных «целевых» стандарта: ГОСТ Р ИСО/МЭК 27006-2020 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности[6] (далее – ГОСТ 27006) и ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности[7] (далее – ГОСТ 27014).

[5] https://base.garant.ru/71730198
[6] http://www.standards.ru/document/6625793.aspx
[7] http://docs.cntd.ru/document/1200112881

Для целей данной публикации отметим в ГОСТ 27006 только основные требования, касающиеся обеспечения компетенций технических экспертов, которые должны обладать специальными знаниями в области технологии, подлежащей аудиту (п. 7.2.1.1.2). Принимая во внимание объект аудита ПХГ, это действительно важно, чтобы аудиторская группа была обеспечена в полной мере необходимой технической адекватностью по многим вопросам – физическая безопасность, системы телекоммуникации и связи, вопросы управления инцидентами ИБ и выполнения полной оценки соответствия. Соответственно, до начала работы руководитель аудиторской группы должен обеспечить, что все аудиторы и технические эксперты (в том числе и внешние) обладают в достаточной мере специальными знаниями, касающимися вопросов, связанных с ИБ, безопасностью процессов и применимого законодательства (п. 7.3.1.1).

Далее отметим важные рекомендации ГОСТ 27006 по анализу мер и средств управления ИБ («контролей», *controls*) на объектах ТЭК. Приложение D представляет руководство по анализу реализованных мер и средств управления ИБ из Приложения А (Annex A) ГОСТ Р ИСО/МЭК 27001 [7] и сбору свидетельств аудита в отношении эффективности этих мер во время аудита. Важно, чтобы свидетельств аудита было достаточно, чтобы сделать вывод об эффективности мер и средств управления ИБ. В таблице D.1 «Классификация мер управления» есть специальное поле D.2.2 "Испытание системы", которое отражает прямую проверку ИТ-систем, функционирующих на объекте ТЭК. Например, для ПХГ это могут быть системы телемеханики, насосные станции, системы SCADA и пр. ГОСТ 27006 определяет 2 категории проверки технических средств контроля: "*возможно*" – т.е. тестирование возможно для оценки, но обычно это не является необходимым и "*рекомендуется*" – т.е. тестирование системы обычно необходимо. В Приложении D ГОСТ 27006 приведены примеры систем, для которых явно рекомендуется тестирование: управление паролями, управление изменениями, контроль технических уязвимостей, распределение ключей и пр.

Для целей данной публикации отметим в ГОСТ 27007 Приложение А «Практическое руководство по аудиту СМИБ», а в данном руководстве обратим внимание на подход к оценке риска ИБ. Здесь следует принять во внимание, что в современном Федеральном законодательстве РФ, применительно к обеспечению безопасности объектов ТЭК, практически нет упоминания рисков и методов менеджмента рисков, соответственно, необходимо применять нормы национальных и международных стандартов, где это определено. В ГОСТ Р ИСО/МЭК 27001 [7] не указан какой-то определенный подход к оценке риска, и аудитор должен проверить, что установленный подход к оценке риска соответствует требованиям к оценке риска, результативен для конкретной организации и соответствует общему подходу к менеджменту риска [10].

В определение подхода включено соответствие правовым и договорным требованиям, а также иным требованиям, важным в отношении рисков и активов, которыми организация должна стратегически управлять, в контексте бизнеса и оценивания риска. Во время аудита ИБ или в составе ИСМ должно быть подтверждено, что подход реализован и выполняется, и результаты оценок риска, полученные в соответствии с применяемым подходом, сопоставимы и воспроизводимы. Аудитор должен подтвердить, что подход позволяет любым сотрудникам, отвечающим за оценку риска, получить одинаковые результаты независимо от того, кто и когда проводит оценку риска, при условии, что они обладают определенным уровнем компетентности в сфере оценки риска и проводят оценки одних и тех же активов в соответствии с процессами и процедурами, определенными в подходе [10]. На критерии принятия риска часто влияют граничные условия, например: политики менеджмента риска конкретной организации, цели, технологии, доступные финансовые средства, соответствующие законы и заинтересованные стороны. Поэтому аудиторам необходимо с должным вниманием проверять эффективность критериев с точки зрения вышеуказанных объектов, подтверждая также, что они определены.

## Цели аудита

С учетом ранее определенных положений и общих требований ISO 19011 [5], сформулируем цели аудита ИБ:

1. Обследование бизнес-процессов, выделенных в рамках проекта «Реализация целевого процесса защиты от утечек конфиденциальной информации» ПХГ;
2. Выявление информационных активов ПХГ, нуждающихся в защите;
3. Создание концептуального понимания принципов легитимного обращения с конфиденциальной информацией в подразделениях ПХГ.

Необходимо отметить, что достижение указанных целей возможно в рамках практического аудита ИБ в соответствии только требованиям ГОСТ Р ИСО/МЭК 27001 [7] или в составе ИСМ.

### План проведения аудита

С учетом ранее определенных положений и общих требований ISO 19011 [5], сформируем обобщенный план проведения аудита ИБ для объектов ПХГ в составе следующих задач:

1. Запрос и анализ документации, регламентирующей обработку и защиту информации на объектах ПХГ;
2. Опрос руководителей подразделений и пользователей в части ведения рабочего процесса, определение защищаемых ресурсов;
3. Инвентаризация рабочих мест с целью определения точного количественного состава технических средств, непосредственно участвующих в процессе обработки защищаемой информации в составе локально-вычислительной сети на объектах ПХГ;
4. Сканирование сети на предмет наличия неучтенных технических средств, определения подсетей, в которых функционирует информационная инфраструктура на объектах ПХГ;
5. Анализ используемых средств защиты на объектах ПХГ;
6. Анализ текущего состояния в соответствии с требованиями Приказа ФСТЭК №31;
7. Анализ текущего состояния в соответствии с требованиями СТО Газпром.

### Ключевые вопросы, выясняемые в процессе интервьюирования

С учетом общих требований ISO 19011 [5], сформируем ключевые вопросы, которые следует выяснить в процессе интервьюирования персонала на объектах ПХГ:

1. Состав бизнес-задач подразделений и обрабатываемые виды информации;
2. Персональная ответственность и владельцы информации;
3. Принципы обращения с информацией (хранение, маркировка грифами, отправка и пр.);
4. Отличительные признаки обрабатываемой информации, наличие примеров или шаблонов;
5. Применяемые опросные листы и их гриф конфиденциальности в качестве свидетельств аудита.

### Программа выполнения аудита ИБ

С учетом ранее определенных положений и общих требований ISO 19011 [5], сформируем пример программы аудита ИБ для ПХГ:

Таблица 1. Программа проведения аудита ИБ

| Сроки проведения | Наименование задачи аудита | Цель | Исполнитель | Выявленные замечания (пример) |
|---|---|---|---|---|
| 10.08.2020 - 14.08.2020 | Подготовка необходимых документов для проведения аудита | Обследование бизнес-процессов, выделенных в рамках проекта «Реализация целевого процесса защиты от утечек конфиденциальной информации» ПХГ | Руководитель Группы аудиторов | |
| 14.08.2020 - | Составление и | Выявление | Группа | |

| | | | | |
|---|---|---|---|---|
| 16.08.2020 | рассылка опросных листов ответственным лицам | информационных активов ПХГ, нуждающихся в защите | аудиторов | |
| 14.08.2020 - 21.08.2020 | Сбор и анализ опросных листов | | Группа аудиторов | |
| 21.08.2020 - 28.08.2020 | Проведение очного интервью специалистов | Создание концептуального понимания принципов легитимного обращения с конфиденциальной информацией в подразделениях ПХГ | Группа аудиторов | |
| 07.09.2020 - 11.09.2020 | Аудит документации по ИБ | Оценка соответствия внутренних нормативных документов | Группа аудиторов | *Требуется обновить отдельные внутренние нормативные документы в силу изменений в законодательстве* |
| 14.09.2020 - 18.09.2020 | Аудит должностных инструкций операторов АРМ | Выявление пробелов в должностных инструкциях | Группа аудиторов | *Инструкции подлежат корректировке. Рекомендации направлены отдельным письмом.* |
| 21.09.2020 - 25.09.2020 | Аудит конфигурации АРМ | Выявление изменения конфигураций АРМ | Группа аудиторов и технических экспертов | *Отдельные АРМ требуют замены в силу своего морального устаревания.* |
| 05.10.2020 - 09.10.2020 | Аудит ПО и ОС АРМ | Проверка актуальности используемых версий ОС и ПО АРМ | Группа аудиторов и технических экспертов | *Х их У АРМ требуют обновления ОС* |
| 12.10.2020 - 16.10.2020 | Аудит системы удалённого доступа | Выявление нарушений в работе системы | Группа аудиторов и технических экспертов | *Имеется система ХХХ, с единой точкой доступа по переназначенному сетевому порту* |
| 19.10.2020 - 23.10.2020 | Аудит сетевой инфраструктуры | Выявление нарушений в работе межсетевого экрана | Группа аудиторов и технических экспертов | *Произведено сегментирование сети на ДМЗ.* |
| 26.10.2020 - 30.10.2020 | Аудит серверной инфраструктуры | Выявление изменений конфигурации серверной инфраструктуры | Группа аудиторов и технических экспертов | *Выявлено Х критических сервера с выходом в “Интернет”* |
| 02.11.2020 - 06.11.2020 | Аудит баз данных | Выявление нарушений | Группа аудиторов и | *ПО Oracle требует обновления* |

| | | | | |
|---|---|---|---|---|
| | | конфиденциальности, целостности и доступности БД | технических экспертов | |
| 02.11.2020 - 06.11.2020 | Аудит каналов передачи ПДн | Проверка используемых каналов передачи, средств передачи | Группа аудиторов и технических экспертов | *Сотрудники иногда использовали почту не рабочего домена для передачи ПДн* |
| 02.11.2020 - 06.11.2020 | Аудит СКУД и СОПС | Проверка работы магнитных ключей и пропусков, соответствия уровней доступа | Группа аудиторов и технических экспертов | *Зафиксирован Х сотрудник с отсутствием магнитного ключа* |
| 09.11.2020 - 13.11.2020 | Аудит системы резервного копирования | Проверка конфиденциальности, целостности и доступности системы резервного копирования | Группа аудиторов и технических экспертов | *Отсутствует доступ к резервным копиям за ХХ год* |
| 09.11.2020 - 13.11.2020 | Аудит системы управления событиями информационной безопасности | Проверка функционирования системы, доступность баз | Группа аудиторов и технических экспертов | *Отсутствуют события с ОС критических серверов Баз Данных, обрабатывающих ПДн.* |
| 16.11.2020 - 20.11.2020 | Аудит настроек СЗИ (в т.ч. матриц доступа) | Проверка актуальности используемых ОС их настроек, сканирование на предмет выявления вредоносного ПО | Группа аудиторов и технических экспертов | *Имеется несоответствие в части предоставляемых сотрудникам прав доступа к БД.*<br>*Обнаружены коллизии доступа.* |
| 23.11.2020 - 30.11.2020 | Анализ полученных результатов | Создание концептуального понимания принципов легитимного обращения с конфиденциальной информацией в подразделениях ПХГ | Группа аудиторов | |
| 23.11.2020 - 30.11.2020 | Составление отчета о текущем положении дел и разработка рекомендаций | | Группа аудиторов | |
| 23.11.2020 - 30.11.2020 | Согласование отчета с заинтересованными лицами и решение спорных вопросов | | Руководитель группы аудиторов | |

## Последовательность выполнения аудита ИБ

С учетом ранее определенных положений и общих требований ISO 19011 [5], сформируем обобщенно последовательность выполнения аудита ИБ для ПХГ (см. рис.1).

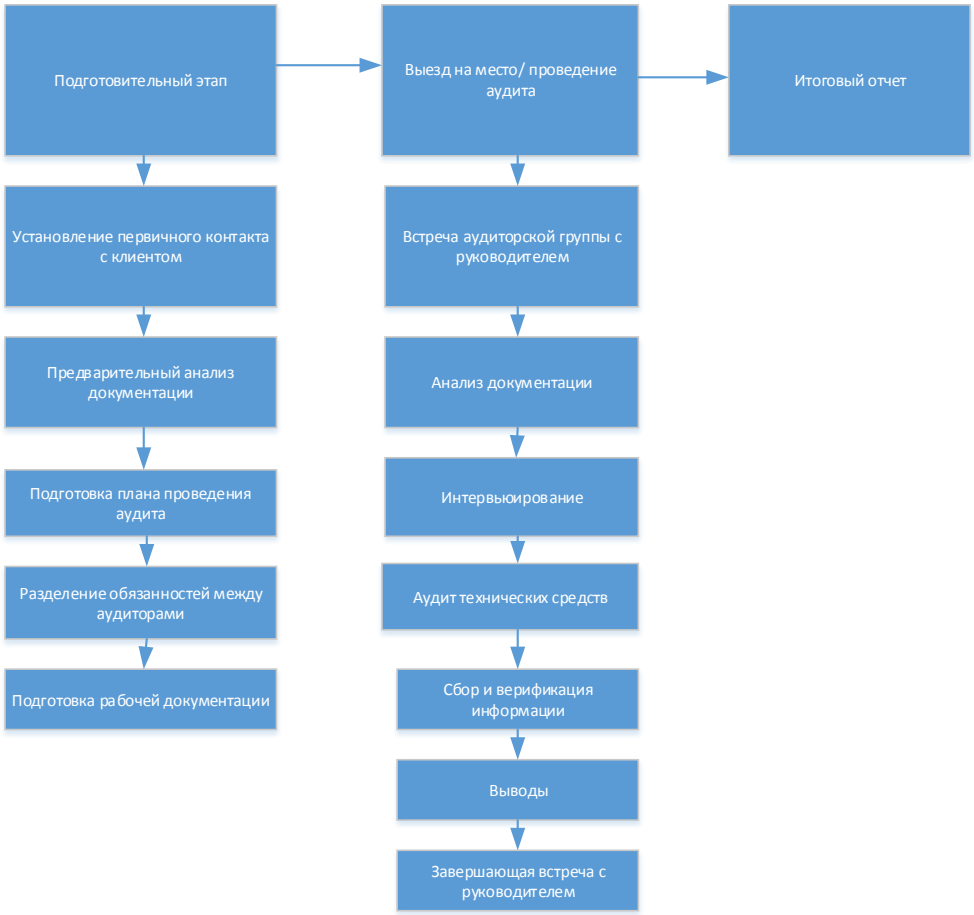


Рисунок 1. — Последовательность аудита ИБ для ПХГ

## Заключение

В представленной публикации кратко рассмотрены аспекты выполнения аудита ИБ на примере объекта ПХГ. Приняты во внимание современные требования к обеспечению безопасности объектов ТЭК, в том числе – Федеральные законы (например, ФЗ-256 и ФЗ-187), актуальные международные ISO (ISO/IEC) и национальные стандарты ГОСТ Р (например, ISO 19011 и ГОСТ Р ИСО/МЭК серии 27000).

Рассмотрена проблема достижения целей аудита ИБ при известных ограничениях по срокам, ресурсам и территориальному охвату, решение которой предлагается в рамках унификации общих концептуальных требования применимого законодательства и лучших практик в области стандартизации аудита ИБ. Показан пример программы аудита ИБ, прошедший практическую апробацию на одном из объектов ПХГ.

Полученные результаты могут найти применение при формировании собственных команд аудиторов и обеспечения заданного уровня безопасности на объектах ТЭК в РФ в современных условиях.

## Литература


1. Лившиц И.И., Танатарова А.Т. Практика применения аудитов систем менеджмента как инструмента оценки и стабилизации экономического состояния предприятия // В сборнике: АРХИТЕКТУРА ФИНАНСОВ: ГЕОПОЛИТИЧЕСКИЕ ДИСБАЛАНСЫ И ПОТЕНЦИАЛ РАЗВИТИЯ НАЦИОНАЛЬНЫХ ФИНАНСОВЫХ СИСТЕМ. сборник материалов VI Международной научно-практической конференции. 2015. С. 80-84.
2. Лившиц И.И., Неклюдов А.В. Методика мгновенных аудитов информационной безопасности // В сборнике: КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ. материалы XXII научно-практической конференции. 2017. С. 139-142.
3. Лившиц И.И. Актуальные вопросы формирования области сертификации интегрированных систем менеджмента для нефтегазовых компаний холдингового типа // Энергобезопасность и энергосбережение. 2020. № 2. С. 43-47.

4. Лившиц И.И. Внедрение систем энергоменеджмента в соответствии с требованиями ISO 50001:2011 для промышленных объектов // Энергобезопасность и энергосбережение. 2014. № 6. С. 9-12.
5. ISO 19011:2018 Guidelines for auditing management systems.
6. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
7. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования;
8. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
9. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности;
10. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
11. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.