

# ISO/IEC 27001 – ПУТЬ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ОСОБЕННОСТИ ВНЕДРЕНИЯ НА ОТЕЧЕСТВЕННЫХ ПРЕДПРИЯТИЯХ



**Дмитриев Александр Анатольевич**  
учредитель, главный редактор  
журнала "Das Management",  
ведущий аудитор ISO 9001, ISO/IEC 27001, BS 25999



В последнее время невозможно представить современный бизнес и процесс управления предприятием без поддержки информационных технологий. Надежные информационные технологии крайне необходимы для работы организации.

Обеспечение безопасности информации и других объектов, относящихся к информации – крайне важная задача для любого бизнеса. Каждый владелец бизнеса и назначенное им руководство уже не может закрывать глаза на текущее состояние информационных систем, они должны видеть и понимать нужды предприятия в информационном обеспечении, решать существующие информационные проблемы. Конечно же, в какой-то мере каждое предприятие уже работает над обеспечением информационной безопасности. Однако этого недостаточно.

Во всеобщем понимании информационная безопасность связана с ограничением доступа третьих лиц к информации. На самом деле это лишь одна из частей общего комплекса вопросов, связанных с информационной безопасностью. Передовые мировые корпорации решают гораздо больший комплекс проблем, связанный с информационной безопасностью. Их работа над безопасностью экономит средства предприятия как в процессе работы, так и за счет нейтрализации неприятных последствий.

Положительным моментом является открытость и доступность международных подходов к обеспечению информационной безопасности на высоком уровне.

Лучшие мировые практики в области управления информационной безопасностью описаны в международном стандарте на системы менеджмента информационной безопасности **ISO/IEC 27001** (ISO 27001). ISO 27001 устанавливает требования к системе менеджмента информационной безопасности (СМИБ) для демонстрации способности организации защищать свои информационные ресурсы.

В данной статье приведена информация о серьезных отличиях отечественного и международного подходов к информационной безопасности.

Понятие «защиты информации» трактуется международным стандартом как обеспечение конфиденциальности, целостности и доступности информации.

С другой стороны, уверен, бывают случаи когда Вы получаете информацию вовремя, но она содержит ошибки. Эти ошибки могут быть вызваны человеческим фактором, сбоем в работе компьютера или другой причиной или целым рядом причин. Этот инцидент показывает пример нарушения **целостности** информации.

Информационная безопасность – ни в коем случае не должна ассоциироваться с параноидальным желанием спрятать, закрыть и удалить коммерческую информацию. Т.к. при таком подходе благие намерения по защите информации приведут как минимум к потере доступности многих информационных ресурсов, что может привести к гораздо более тяжелым финансовым последствиям, чем их утечка. Всегда нужно помнить о разумном равновесии, обеспечивая одновременно все три свойства – конфиденциальность, целостность, доступность. При этом, всегда нужно понимать единственно правильную цель работы предприятия. Эта цель не может быть рассмотрена в плоскости лучшей оснащенности оборудованием или высокой компетентности персонала. Единственная цель предприятия – получение финансовых выгод. Исключения могут составлять благотворительные и подобные им организации.

Рассмотрим основные понятия современного подхода к информационной безопасности.

Основным объектом стандарта является **Информационный актив**

Что такое **Информационный актив**?

Это материальный или нематериальный объект, который:

- является информацией или содержит информацию,
- служит для обработки, хранения или передачи информации,
- имеет ценность для организации.



Примерами информационных активов могут быть: договора с клиентами, финансовая отчетность, технологическая карта, журнал регистрации писем, проекты новых продуктов или услуг, ноутбук с информацией о финансовом состоянии предприятия, сервер с информацией о клиентах, архив (помещение) с бумажными делами сотрудников предприятия, руководитель предприятия с планом перспективной и оперативной деятельности.

Информационные активы обладают основными свойствами финансовых и материальных активов предприятия: стоимость, ценность для организации, возможность накопления, возможность трансформации в другие активы. Зачастую ценность информационного актива предприятия превосходит ценность всех финансовых. Примером такого актива является имидж предприятия.

Сегодняшние реалии таковы, что и финансовые, и материальные, и информационные активы нуждаются в защите. Надежная защита информационных активов существенна для работы предприятия. Поэтому несоответствующий уровень защиты – часто недооцененный фактор риска, который может стать угрозой для существования.

Чтобы достичь уровня информационной безопасности, который удовлетворяет потребности, необходимо больше, чем просто купить антивирусное ПО, системы сетевой защиты или системы резервирования данных. Необходима четкая и слаженная система.

Для того, чтобы принять или отвергнуть стандарт, в котором описана надежная система информационной безопасности, предлагаю познакомиться с выгодами, которые вытекают из реализации требований стандарта.



Рис. 1. Свойства информации (информационных активов)

Важно отметить, что, кроме привычной нам конфиденциальности стандарт четко указывает на обязательность работы над другими, зачастую более важными свойствами. Эти свойства – доступность и целостность.

Рассмотрим живые примеры. Вы на своем рабочем месте, выполняя функциональные обязанности, зачастую поздно получаете информацию от своего подчиненного или соседнего подразделения. Естественно, в результате это отражается на вашем рабочем процессе. Этот инцидент показывает пример нарушения **доступности** ин-

## МЕЖДУНАРОДНЫЕ, ЕВРОПЕЙСКИЕ, ОТРАСЛЕВЫЕ СТАНДАРТЫ И ДИРЕКТИВЫ

### ВЫГОДЫ ВНЕДРЕНИЯ СТАНДАРТА

Прежде чем приступать к внедрению требований стандарта важно понимать выгоды, которые получит предприятие. Ниже приведен перечень выгод, среди которых возможно будут найдены подходящие конкретному предприятию.

1. Уменьшается и оптимизируется стоимость поддержки системы безопасности. Вы будете тратить деньги только на те направления безопасности, которые закроют самые опасные риски для Вашего конкретного предприятия. Объективная оценка сочетаний «ущерб-вероятность» позволит постоянно эффективно финансировать информационную безопасность (рис. 2).



Рис. 2. Схема принятия решения о финансировании информационной безопасности

2. Информационные активы станут понятными для менеджмента компании. Стандарт требует создания и поддержания в актуальном состоянии перечня информационных активов.

3. Угрозы и уязвимости безопасности для существующих бизнес-процессов будут регулярно выявляться.

4. Риски будут просчитываться и решения будут приниматься на основе бизнес-целей компании, в первую очередь финансовых целей.

5. Управление информационными активами предприятия в критичных ситуациях будет эффективным благодаря разработке, внедрению и тестированию планов по восстановлению бизнеса.

6. Будет проводиться процесс выполнения политики безопасности (находить и исправлять слабые места в системе информационной безопасности в регулярном режиме).

7. Будет обеспечена прозрачность и чистота бизнеса перед законом благодаря соответствию стандарту.

8. Появится надежная защита от рейдерских атак.  
9. Подсистема информационной безопасности интегрируется в общую систему менеджмента.

10. Предприятие получит международное признание и повысится его авторитет, как на внутреннем рынке, так и на внешних рынках.

### ЯЗЫК СТАНДАРТА ПРОСТ И СЛОЖЕН

Стандарт состоит из четырех частей.

**Первая часть** «Общие положения» содержит информацию о предназначении стандарта, его связи с другими стандартами по ИБ, а также термины и определения.

**Вторая часть** «Требования к СМИБ» является основной. Она выдвигает обязательные для выполнения требования к СМИБ и позволяет на их основе построить эффективную систему.

Общие требования размещаются всего на девяти страницах и разделены на следующие разделы:

4. Система менеджмента информационной безопасности
5. Обязательства руководства
6. Внутренние аудиты СМИБ
7. Анализ СМИБ руководством
8. Совершенствование СМИБ

**Третья часть** стандарта называется «Приложение А. Цели и меры контроля». Эта часть описывает конкретные требования к каждому направлению информационной безопасности. Всего 11 направлений, которые обозначены в соответствии с разделами 5-15 стандарта ISO/IEC 17799:2005. Стандарт ISO/IEC 17799:2005 содержит рекомендации по реализации требований "Приложения А" стандарта ISO/IEC 27001:2005. Требования «Приложения А» являются обязательными для выполнения, но стандарт позволяет исключить направления, которые не возможно применить на предприятии.

Стандарт достаточно удобно читать, понимать и применять на практике. Рассмотрим для примера пункт 4.2.1, в котором речь идет о построении системы менеджмента информационной безопасности. Для удобства расположим строки этого пункта в виде ступеней для подъема вверх. Проходя каждую ступень мы поднимаемся выше к созданию эффективной системы (рис. 3).



Рис. 3. Фрагмент стандарта ISO/IEC 27001:2005: пункт 4.2.1

Некоторые пункты стандарта являются поистине сложными для восприятия и понимания. Для детального знакомства со стандартом рекомендуем использовать дополнительные литературные источники, базирующиеся на стандарте ISO/IEC 27001. Кроме этого наиболее

эффективным способом изучения стандарта являются специализированные учебные курсы, которые предлагают в странах бывшего СССР международные сертификационные общества и их партнеры.

# МЕЖДУНАРОДНЫЕ, ЕВРОПЕЙСКИЕ, ОТРАСЛЕВЫЕ СТАНДАРТЫ И ДИРЕКТИВЫ

## КАК РАБОТАЕТ СТАНДАРТ?

Чтобы понять как работает стандарт рассмотрим достаточно простую схему, представляющую его основу (см. рис. 4).



Рис. 4. Общая схема работы эффективной системы управления информационной безопасностью

Схема работает в три этапа. **На первом этапе** строятся управленческие процессы. Среди них самым важным является процесс управления рисками. Управленческие процессы в регулярном режиме закрутят механизм отслеживания и оценки существующих и вновь появляющихся рисков. В результате реализации первого этапа мы сможем видеть все риски и выделять наиболее серьезные для нашего бизнеса. Другими словами, мы четко определим, чего мы должны опасаться. Когда мы знаем, что нам угрожает, мы должны перебрать все направления безопасности, которые могут привести к возникновению на практике тех самых опасных рисков. Эти направления перечислены в стандарте в Приложении А. Наряду с элементами управления для компьютеров и компьютерных сетей в стандарте уделяется большое внимание вопросам разработки политики безопасности, работе с персоналом (прием на работу, обучение, увольнение с работы), обеспечению непрерывности производственного процесса, юридическим требованиям.

**Второй этап работы** схемы заключается в четком определении направлений информационной безопасности. Всего их 131, но для простоты и удобства они сгруппированы в 11 групп (рис.5).

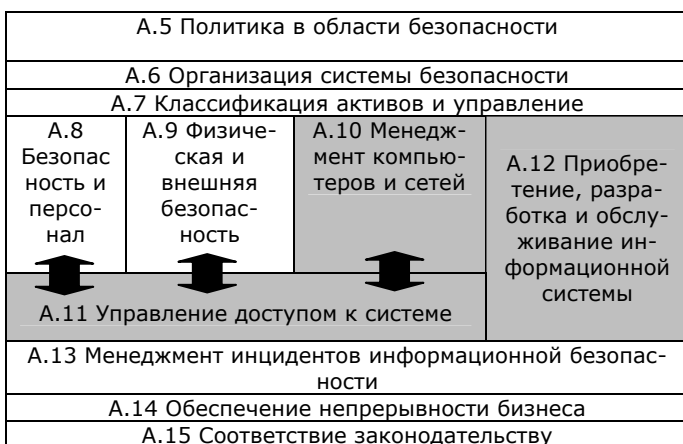


Рис. 5. Направления информационной безопасности

В результате реализации второго этапа мы будем знать по каким направлениям возможно или необходимо обеспечивать информационную безопасность. Либо это будут направления, связанные с персоналом, или физической защитой, или компьютерной техникой. Украинские традиции таковы, что данные направления не определяются объективно, с учетом важности того или иного направления. Служба ИТ как правило просит средства только на компьютерную технику, в то время как гораздо эффективнее и менее затратно

вкладывать средства в повышение компьютерной грамотности персонала. На данном этапе завершается главная роль стандарта ISO 27001.

**Третий этап** – технический. Для его реализации не существует единой методики или стандарта. В этот момент каждое предприятие исходя из своих финансовых возможностей принимает решение либо о покупке техники, ПО, обучении персонала, усилении пропускного режима или выбирает другие меры.

На этом этапе выбираются конкретные поставщики конкретных мероприятий.

В результате реализации данной схемы достигается экономический эффект от вложений в информационную безопасность. Без этой схемы, прибегая сразу же к покупке антивирусов, компьютеров и других средств, предприятие обречено на необъективность затрат.

После принятия решения о внедрении системы менеджмента информационной безопасности представитель предприятия стоит перед выбором: самостоятельно внедрять систему, либо пригласить консультанта. Однозначной рекомендации в этом случае быть не может. Многое зависит от финансовых возможностей предприятия, статуса ответственного за внедрение системы менеджмента и других параметров. Также, к сожалению, не существует единого алгоритма внедрения системы. Вы не найдете его ни в одном стандарте. С одной стороны Вы вольны в выборе плана действий. С другой стороны Вы понимаете, что уже где-то и у кого-то существует шаблонный проверенный вариант. Поэтому не будем сочинять высокопарные оды авторитетным консультантам по информационной безопасности. Приведем реальный пример алгоритма, опробованный в странах бывшего СССР.

### АЛГОРИТМ ВНЕДРЕНИЯ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ МЕЖДУНАРОДНОГО СТАНДАРТА ISO/IEC 27001

#### Первый этап. Управленческий

- Осознать цели и выгоды внедрения СМИБ
- Получить поддержку руководства на внедрение и ввод в эксплуатацию системы менеджмента информационной безопасности (СМИБ)
- Распределить ответственность по СМИБ

#### Второй этап. Организационный

- Создать группу по внедрению и поддержке СМИБ
- Обучить группу по внедрению и поддержке СМИБ
- Определить область действия СМИБ

#### Третий этап. Первоначальный анализ СМИБ

- Провести анализ существующей СМИБ
- Определить перечень работ по доработке существующей СМИБ

## **МЕЖДУНАРОДНЫЕ, ЕВРОПЕЙСКИЕ, ОТРАСЛЕВЫЕ СТАНДАРТЫ И ДИРЕКТИВЫ**

### **Четвертый этап. Определение политики и целей СМИБ**

- Определить политику СМИБ
- Определить цели СМИБ по каждому процессу СМИБ

### **Пятый этап. Сравнение текущей ситуации со стандартом**

- Провести обучение ответственных за СМИБ требованиям стандарта
- Проработать требования стандарта
- Сравнить требования стандарта с существующим положением дел

### **Шестой этап. Планирование внедрения СМИБ**

- Определить перечень мероприятий для достижения требований стандарта
- *Разработать руководство по информационной безопасности*

### **Седьмой этап. Внедрение системы управления рисками**

- Разработать процедуру по идентификации рисков
- Идентифицировать и ранжировать активы (каталог «Модули» методики ИТ-Грундшутц)
- Определить ответственных за активы
- Оценить активы
- Идентифицировать угрозы и уязвимости активов (каталог «Угрозы» методики ИТ-Грундшутц)
- Рассчитать и ранжировать риски
- Разработать план по снижению рисков (каталог «Меры защиты» методики ИТ-Грундшутц)
- Определить неприменимые контроли (направления) безопасности из приложения А
- Разработать положение о применимости контролей

### **Восьмой этап. Разработка документации СМИБ**

- Определить перечень документов (процедур, записей, инструкций) для разработки
- Разработка процедур и других документов
- Разработка и введение в действие документов СМИБ

### **Девятый этап. Обучение персонала**

- Обучение руководителей подразделений требованиям ИБ
- Обучение всего персонала требованиям ИБ

### **Десятый этап. Разработка и принятие мер по обеспечению работы СМИБ**

- Внедрение средств защиты (административных, учебных, технических)

### **Одиннадцатый этап. Внутренний аудит СМИБ**

- Подбор команды внутреннего аудита СМИБ
- Планирование внутреннего аудита СМИБ
- Проведение внутреннего аудита СМИБ

### **Двенадцатый этап. Анализ СМИБ со стороны высшего руководства**

- Проведение анализа СМИБ со стороны высшего руководства

### **Тринадцатый этап. Официальный запуск СМИБ**

- Приказ о введении в действие СМИБ

### **Четырнадцатый этап. Оповещение заинтересованных сторон**

- Информирование клиентов, партнеров, СМИ о запуске СМИБ

Данный алгоритм содержит некоторые этапы, которые не обязательны для реализации. Эти этапы выделены подчеркнутым текстом. Также в данном алгоритме присутствуют рекомендации по использованию немецких каталогов "ИТ-Грундшутц". Используя эти каталоги, Вы можете избавиться от большей части рутинных операций. Данные каталоги являются бесплатными и размещены на интернет-сайте немецкого федерального бюро по информационной безопасности "[www.bsi.de](http://www.bsi.de)". Отрицательной стороной является то, что каталоги "ИТ-Грундшутц" предлагаются на немецком и английском языках.

## **ОСОБЕННОСТИ ВНЕДРЕНИЯ ТРЕБОВАНИЙ СТАНДАРТА НА ОТЕЧЕСТВЕННЫХ ПРЕДПРИЯТИЯХ**

Стандарт ISO 27001 содержит ряд требований, которые достаточно сложно выполнить, учитывая отечественный менталитет сотрудников и руководства, исторические особенности становления и развития предприятия. Для построения эффективной системы управления информационной безопасностью необходимо выполнить абсолютно все требования. Исходя из собственного опыта, отзывов отечественных аудиторов и экспертов приведем некоторые сложные требования стандарта.

### **Стандарт требует:**

1. Наличия налаженных контактов с различными инстанциями, работающими в Украине в области информационной безопасности.

Таковыми могут быть силовые структуры – МВД и СБУ, консалтинговые фирмы, работающие в области безопасности, сертификационные общества, форумы по информационной безопасности.

2. Наличие независимого пересмотра (надзора) системы менеджмента информационной безопасности. Для этого можно привлечь сертификационный орган, консалтинговую компанию либо представителей предприятия-партнера.

3. Наличие актуального и полного реестра информационных активов предприятия. Это остаточной большой объем работ и многие предприятия «запускают» актуализацию реестра.

4. Требования по информационной безопасности должны применяться и выполняться при приеме абсолютно всего персонала на работу. Это могут быть требования о несудимости, о наличии компьютерных навыков, личностные качества.

5. Во время работы весь персонал периодически должен проходить обучение или инструктаж по информационной безопасности.

6. При увольнении сотрудника должны быть четко проверены по реестру и возвращены все информационные активы, которые были доступны ему во время работы.

7. Физическая безопасность предприятия не должна ограничиваться сохранностью материальных активов. В рамках физической безопасности должны быть решены проблемы с утечкой или повреждением нематериальных информационных активов.

8. При разработке программного обеспечения для собственных нужд необходимо разделять среду разработки, тестирования и эксплуатации программного обеспечения. Другими словами, запрещается разрабатывать программный продукт и работать с ним на одном компьютере. Возможно понадобится приобрести новые компьютеры для реализации данного требования.

9. Должны быть разработаны и должны выполняться требования по информационной безопасности для услуг третьих сторон. Таких как Интернет-провайдер, консультанты, технические специалисты других предприятий.

10. Любое устройство, содержащее информацию, перед отправкой в ремонт, на склад, в утилизацию должно быть обработано с точки зрения удаления всей имеющейся на нем информации.

11. Системная документация ко всему оборудованию, имеющему отношение к информации должна быть в наличии, должна быть доступна в нужный момент времени и не должна быть доступна третьим лицам.

12. Необходимо учитывать требования по информационной безопасности не только к компьютерным информационным системам, но к простым факсам, телетайпам и телефонам.

13. Все действия системных администраторов должны фиксироваться. Это особенно сложный пункт. Но его необходимость продиктована тем, что системные администраторы по роду своей деятельности постоянно корректируют (конфигурируют) настройки информационных систем. Уход с работы подобного сотрудника приведет к серьезным финансовым последствиям для предприятия. Наличие записей о проделанных работах поможет новому системному администратору оперативно получить управление информационной системой и решать задачи по ремонту и наладке системы.

14. На всем предприятии должна применяться политика чистого рабочего стола (мебель) и экрана компьютера. Т.к. именно таким образом происходит большое количество утечек информации.

15. Все инциденты, другими словами все проблемы, связанные с информацией (поломка компьютера, кража оборудования, кража информации, сбой в работе информационной системы и др.) должны фиксироваться в едином реестре инцидентов. Эта работа даст возможность объективно оценить существующий уровень проблем.

16. На предприятии должны быть разработаны планы по восстановлению бизнеса. Камнем преткновения зачастую является их обязательное тестирование.

17. Предприятие должно соблюдать требования закона «Об авторских и смежных правах». Т.е. следуя стандарту предприятие не может использовать нелегальное программное обеспечение.

18. На предприятии полностью должны быть устранены случаи нецелевого использования средств обработки информации. Т.е. запрещены игры, частные прогулки по Интернету, поиск рефератов и др.

Это практически полный список сложных для реализации требований стандарта. Другие требования достаточно просты для понимания и реализации.

*Данная статья предназначена для знакомства представителей предприятий с международным подходом к информационной безопасности. Особенное внимание обращено на проблемные места, возникающие при внедрении международного подхода на отечественных предприятиях.*