
ВАДИМ ГРЕБЕННИКОВ

# УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

СТАНДАРТЫ СУИБ

Вадим Гребенников

# Управление информационной безопасностью. Стандарты СУИБ

«Издательские решения»

**Гребенников В.**

Управление информационной безопасностью. Стандарты СУИБ / В. Гребенников — «Издательские решения»,

ISBN 978-5-4493-0690-6

Книга рассказывает о семействе международных стандартов ISO/IEC 27k, определяющих требования и правила СУИБ (системы управления информационной безопасностью), порядок разработки СУИБ и алгоритмы управления рисками информационной безопасности и инцидентами информационной безопасности. Официальная веб-страница автора: http://cryptohistory.ru

ISBN 978-5-4493-0690-6

# Содержание

# Управление информационной безопасностью Стандарты СУИБ

## Вадим Гребенников



ISBN 978-5-4493-0690-6
Создано в интеллектуальной издательской системе Ridero

# 1. Семейство стандартов управления информационной безопасностью

## 1.1. История развития стандартов управления информационной безопасностью

Сегодня безопасность цифрового пространства показывает новый путь национальной безопасности каждой страны. В соответствии с ролью информации как ценного товара в бизнесе, её защита, безусловно, необходима. Для достижения этой цели, каждой организации, в зависимости от уровня информации (с точки зрения экономической ценности), требуется разработка системы управления информационной безопасностью (далее – СУИБ), пока существует возможность, защиты своих информационных активов.

В организациях, существование которых значительно зависит от информационных технологий (далее – ИТ), могут быть использованы все инструменты для защиты данных. Тем не менее, безопасность информации необходима для потребителей, партнеров по сотрудничеству, других организаций и правительства. В связи с этим, для защиты ценной информации, необходимо что бы каждая организация стремилась к той или иной стратегии и реализации системы безопасности на её основе.

СУИБ является частью комплексной системы управления, основанной на оценке и анализов рисков, для разработки, реализации, администрирования, мониторинга, анализа, поддержания и повышения информационной безопасности (далее – ИБ) и ее реализации, полученных из целей организации и требования, требования безопасности, используемых процедур и размерах и структуре ее организации.

Зарождение принципов и правил управления ИБ началось в Великобритании в 1980-х годах. В те годы Министерство торговли и промышленности Великобритании (англ. Department of Trade and Industry, DTI) организовало рабочую группу для разработки свода лучших практик по обеспечению ИБ.

В 1989 году «DTI» опубликовало первый стандарт в этой области, который назывался PD 0003 «Практические правила управления ИБ». Он представлял собой перечень средств управления безопасностью, которые в то время считались адекватными, нормальными и хорошими, применимыми как к технологиям, так и средам того времени. Документ «DTI» был опубликован как руководящий документ британской системы стандартов (англ. British Standard, BS).

В 1995 году Британский институт стандартов (англ. British Standards Institution, BSI) принял национальный стандарт BS 7799—1 «Практические правила управления ИБ». Она описывал 10 областей и 127 механизмов контроля, необходимых для построения СУИБ (англ. Information Security Management System, ISMS), определенных на основе лучших примеров из мировой практики.

Этот стандарт и стал прародителем всех международных стандартов СУИБ. Как и любой национальный стандарт BS 7799 в период 1995—2000 годов пользовался, скажем так, умеренной популярностью только в рамках стран британского содружества.

В 1998 году появилась вторая часть этого стандарта – BS 7799—2 «СУИБ. Спецификация и руководство по применению», определившая общую модель построения СУИБ и набор обязательных требований, на соответствие которым должна производиться сертификация. С появлением второй части BS 7799, определившей, что должна из себя представлять СУИБ, началось активное развитие системы сертификации в области управления безопасностью.

В конце 1999 года эксперты Международной организации по стандартизации (англ. International Organization for Standardization, ISO) и Международной электротехнической комиссии (англ. International Electrotechnical Commission, IEC) пришли к выводу, что в рамках существующих стандартов отсутствует специализированный стандарт управления ИБ. Соответственно, было принято решение не заниматься разработкой нового стандарта, а по согласованию с «BSI», взяв за базу BS 7799—1, принять соответствующий международный стандарт ISO/IEC.

В конце 1999 года обе части BS 7799 были пересмотрены и гармонизированы с международными стандартами систем управления качеством ISO/IEC 9001 и экологией ISO/IEC 14001, а год спустя без изменений BS 7799—1 был принят в качестве международного стандарта ISO/IEC 17799:2000 «Информационные технологии (далее – ИТ). Практические правила управления ИБ».

В 2002 году была обновлена и первая часть стандарта BS 7799—1 (ISO/IEC 17799), и вторая часть BS 7799—2.

Что же касается официальной сертификации по ISO/IEC 17799, то она изначально не была предусмотрена (полная аналогия с BS 7799). Была предусмотрена только сертификация по BS 7799—2, который представлял собой ряд обязательных требований (не вошедших в BS 7799—1) и в приложении перечень условно обязательных (на усмотрение сертификатора) наиболее важных требований BS 7799—1 (ISO/IEC 17799).

На территории СНГ первой страной, которая в ноябре 2004 года приняла стандарт ISO/IEC 17799:2000 в качестве национального, была Беларусь. Россия ввела этот стандарт только в 2007 году. Центральный Банк РФ на его базе создал стандарт управления ИБ для банковской сферы РФ.

В составе ISO/IEC за разработку семейства международных стандартов по управлению ИБ отвечает подкомитет №27, поэтому была принята схема нумерации данного семейства стандартов с использованием серии последовательных номеров, начиная с 27000 (27k).

В 2005 году подкомитет SC 27 «Методы защиты ИТ» Объединенного технического комитета JTC 1 «ИТ» ISO/IEC разработал сертификационный стандарт ISO/IEC 27001 «ИТ. Методы защиты. СУИБ. Требования», пришедший на смену BS 7799—2, и теперь сертификация проводится уже по ISO 27001.

В 2005 году на основе ISO/IEC 17799:2000 был разработан ISO/IEC 27002:2005 «ИТ. Методы защиты. Свод норм и правил управления ИБ».

В начале 2006 года был принят новый британский национальный стандарт BS 7799—3 «СУИБ. Руководство по управлению рисками ИБ», который в 2008 году получил статус международного стандарта ISO/IEC 27005 «ИТ. Методы защиты. Управление рисками ИБ».

В 2004 году Британским институтом стандартов был опубликован стандарт ISO/IEC TR 18044 «ИТ. Методы защиты. Управление инцидентами ИБ». В 2011 году на его базе был разработан стандарт ISO/IEC 27035 «ИТ. Методы защиты. Управление инцидентами ИБ».

В 2009 году был принят стандарт ISO/IEC 27000 «ИТ. СУИБ. Общий обзор и терминология». Он предоставляет обзор систем управления ИБ и определяет соответствующие термины. Словарь тщательно сформулированных формальных определений охватывает большинство специализированных терминов, связанных с ИБ и используемых в стандартах группы ISO/IEC 27.

25 сентября 2013 года были опубликованы новые версии стандартов ISO/IEC 27001 и 27002. С этого момента стандарты серии ISO/IEC 27k (управление ИБ) полностью интегрированы со стандартами серии ISO/IEC 20k (управление ИТ-сервисами). Вся терминология из ISO/IEC 27001 перенесена в ISO/IEC 27000, который определяет общий терминологический аппарат для всего семейства стандартов ISO/IEC 27k.

## 1.2. Стандарт ISO/IEC 27000—2014

Последнее обновление стандарта ISO/IEC 27000 «ИТ. СУИБ. Общий обзор и терминология» состоялось 14 января 2014 года.

*Стандарт состоит из следующих разделов:*

– введение;
– сфера применения;
– термины и определения;
– системы управления ИБ;
– семейство стандартов СУИБ.

# Введение

***Обзор***

Международные стандарты системы управления представляют модель для налаживания и функционирования системы управления. Эта модель включает в себя функции, по которым эксперты достигли согласия на основании международного опыта, накопленного в этой области.

При использовании семейства стандартов СУИБ организации могут реализовывать и совершенствовать СУИБ и подготовиться к ее независимой оценке, применяемой для защиты информации, такой как финансовая информация, интеллектуальная собственность, информация о персонале, а также информация, доверенная клиентами или третьей стороной. Эти стандарты могут использоваться организацией для подготовки независимой оценки своей СУИБ, применяемой для защиты информации.

***Семейство стандартов СУИБ***

Семейство стандартов СУИБ, имеющее общее название «Information technology. Security techniques» (Информационная технология. Методы защиты), предназначено для помощи организациям любого типа и размера в реализации и функционировании СУИБ и состоит из следующих международных стандартов:

– ISO/IEC 27000 СУИБ. Общий обзор и терминология;

– ISO/IEC 27001 СУИБ. Требования;

– ISO/IEC 27002 Свод правил по управлению ИБ;

– ISO/IEC 27003 Руководство по реализации СУИБ;

– ISO/IEC 27004 УИБ. Измерения;

– ISO/IEC 27005 Управление рисками ИБ;

– ISO/IEC 27006 Требования для органов, обеспечивающих аудит и сертификацию СУИБ;

– ISO/IEC 27007 Руководство по проведению аудита СУИБ;

– ISO/IEC TR 27008 Руководство по аудиту механизмов контроля ИБ;

– ISO/IEC 27010 УИБ для межсекторных и межорганизационных коммуникаций;

– ISO/IEC 27011 Руководство по УИБ для телекоммуникационных организаций на основе ISO/IEC 27002;

– ISO/IEC 27013 Руководство по интегрированной реализации стандартов ISO/IEC 27001 и ISO/IEC 20000—1;

– ISO/IEC 27014 Управление ИБ высшим руководством;

– ISO/IEC TR 27015 Руководство по УИБ для финансовых сервисов;

– ISO/IEC TR 27016 УИБ. Организационная экономика;

*– ISO/IEC 27035 Управление инцидентами ИБ (в стандарте не указан).*

*Международный стандарт, не имеющие этого общего названия:*

– ISO 27799 Информатика в здравоохранении. УИБ по стандарту ISO/IEC 27002.

***Цель стандарта***

Стандарт предоставляет обзор СУИБ и определяет соответствующие условия.

*Семейство стандартов СУИБ содержит стандарты, которые:*

– определяют требования к СУИБ и сертификации таких систем;

– содержат прямую поддержку, детальное руководство и разъяснение целого процесса создания, внедрения, сопровождения и улучшения СУИБ;

– включают в себя отраслевые руководящие принципы для СУИБ;

– руководят проведением оценки соответствия СУИБ.

**1. Сфера применения**

Стандарт предосталяет обзор СУИБ, а также условий и определений, широко использующихся в семействе стандартов СУИБ. Стандарт применим ко всем типам и размерам организаций (например, коммерческие предприятия, правительственные учреждения, неприбыльные организации).

**2. Термины и определения**

*Раздел содержит определение 89 терминов, например:*

– *информационная система* – приложения, сервисы, ИТ активы и другие компоненты обработки информации;

– *информационная безопасность (ИБ)* – сохранение конфиденциальности, целостности и доступности информации;

– *доступность* – свойство быть доступным и готовым к использованию по запросу уполномоченного лица;

– *конфиденциальность* – свойство информации быть недоступной или закрытой для неуполномоченных лиц;

– *целостность* – свойство точности и полноты;

– *неотказуемость* – способность удостоверять наступление события или действие и их создающих субьектов;

– *событие ИБ* – выявленное состояние системы (сервиса или сети), указывающее на возможное нарушение политики или мер ИБ, или прежде неизвестная ситуация, которая может касаться безопасности;

– *инцидент ИБ* – одно или несколько событий ИБ, которые со значительной степенью вероятности приводят к компрометации бизнес-операций и создают угрозы для ИБ;

– *управление инцидентами ИБ* – процессы обнаружения, оповещения, оценки, реагирования, рассмотрения и изучения инцидентов ИБ;

– *система управления* – набор взаимосвязанных элементов организации для установления политик, целей и процессов для достижения этих целей;

– *мониторинг* – определение статуса системы, процесса или действия;

– *политика* – общее намерение и направление, официально выраженное руководством;

– *риск* – эффект неопределенности в целях;

– *угроза* – возможная причина нежелательного инцидента, который может нанести ущерб;

– *уязвимость* – недостаток актива или меры защиты, которое может быть использовано одной или несколькими угрозами.

**3. Системы управления ИБ**

*Раздел «СУИБ» состоит из следующих основных пунктов:*

– описание СУИБ;

– внедрение, контроль, сопровождение и улучшение СУИБ;

– преимущества внедрения стандартов семейства СУИБ.

**3.1. Введение**

*Организации всех типов и размеров:*

– собирают, обрабатывают, хранят и передают информацию;

– осознают, что информация и связанные процессы, системы, сети и люди являются важными активами для достижения целей организации;

– сталкиваются с целым рядом рисков, которые могут повлиять на функционирование активов;

– устраняют предполагаемый риск посредством внедрения мер и средств ИБ.

Вся информация, хранимая и обрабатываемая организацией, является объектом для угроз атаки, ошибки, природы (например, пожар или наводнение) и т. п. и объектом уязвимостей, свойственных ее использованию.

Обычно понятие ИБ базируется на информации, которая рассматривается как имеющий ценность актив и требует соответствующей защиты (например, от потери доступности, конфиденциальности и целостности). Возможность получить своевременный доступ уполномоченных лиц к точной и полной информации является катализатором бизнес-эффективности.

Эффективная защита информационных активов путем определения, создания, сопровождения и улучшения ИБ является необходимым условием для достижения организацией своих целей, а также поддержания и улучшения правового соответствия и репутации. Эти координированные действия, направленные на внедрение надлежащих мер защиты и обработку неприемлемых рисков ИБ, общеизвестны как элементы управления ИБ.

*По мере изменения рисков ИБ и эффективности мер защиты в зависимости от меняющихся обстоятельств организации следует:*

– контролировать и оценивать эффективность внедренных мер и процедур защиты;

– идентифицировать возникающие риски для обработки;

– выбирать, внедрять и улучшать соответствующие меры защиты надлежащим образом.

Для взаимосвязи и координации действий ИБ каждой организации следует сформировать политику и цели ИБ и эффективно достигать этих целей, используя систему управления.

**3.2. Описание СУИБ**

*Описание СУИБ предусматривает следующие составляющие:*

– положения и принципы;

– информация;

– информационная безопасность;

– управление;

– система управления;

– процессный подход;

– важность СУИБ.

***Положения и принципы***

СУИБ состоит из политик, процедур, руководств и соответствующих ресурсов и действий, коллективно управляемых организацией, для достижения защиты своих информационных активов. СУИБ определяет систематический подход к созданию, внедрению, обработке, контролю, пересмотру, сопровождению и улучшению ИБ организации для достижения бизнес-целей.

Она базируется на оценке риска и приемлемых уровнях риска организации, разработанных для эффективной обработки и управления рисками. Анализ требований защиты информационных активов и применение соответствующих мер защиты, чтобы обеспечить необходимую защиту этих активов, способствует успешной реализации СУИБ.

*Следующие основные принципы способствуют успешной реализации СУИБ:*

– понимание необходимости системы ИБ;

– назначение ответственности за ИБ;

– объединение обязательств руководства и интересов заинтересованных лиц;

– возрастание социальных ценностей;

– оценки риска, определяющие соответствующие меры защиты для достижения допустимых уровней риска;

– безопасность как неотъемлемый элемент ИС и сетей;

– активное предупреждение и выявление инцидентов ИБ;

– обеспечение комплексного подхода к УИБ;

– непрерывная переоценка и соответствующее улучшение ИБ.

***Информация***

Информация – это актив, который наряду с другими важными бизнес-активами важен для бизнеса организации и, следовательно, должен быть соответственно защищен. Информация может храниться в различных формах, включая такие как цифровая форма (например, файлы с данными, сохраненные на электронных или оптических носителях), материальная форма (например, на бумаге), а также в нематериальном виде в форме знаний сотрудников.

Информация может быть передана различными способами, включая курьера, электронную или голосовую коммуникацию. Независимо от того, в какой форме представлена информация и каким способом передается, она должна быть должным образом защищена.

Во многих организациях информация зависит от информационной и коммуникационной технологии. Эта технология является существенным элементом в любой организации и облегчает создание, обработку, хранение, передачу, защиту и уничтожение информации.

***Информационная безопасность***

ИБ включает в себя три основных измерения (свойства): конфиденциальность, доступность и целостность. ИБ предусматривает применение и управление соответствующими мерами безопасности, которые включают в себя рассмотрение широкого диапазона угроз, с целью обеспечения длительного успеха и непрерывности бизнеса и минимизации влияний инцидентов ИБ.

ИБ достигается применением соответствующего набора мер защиты, определенного с помощью процесса управления рисками и управляемого с использованием СУИБ, включая политики, процессы, процедуры, организационные структуры, программные и аппаратные средства, чтобы защитить идентифицированные информационные активы.

Эти меры защиты должны быть определены, реализованы, проконтролированы, проверены и при необходимости улучшены, чтобы гарантировать, что уровень ИБ соответствует бизнес-целям организации. Соответствующие меры и средства ИБ следует органично интегрировать в бизнес-процессы организации.

***Управление***

Управление включает в себя действия по руководству, контролю и непрерывному совершенствованию организации в рамках соответствующих структур. Управленческая деятельность включает в себя действия, методы или практику формирования, обработки, направления, наблюдения и контроля ресурсов. Величина управленческой структуры может варьироваться от одного человека в небольших организациях до управленческой иерархии в крупных организациях, состоящих из многих людей.

Относительно СУИБ управление включает в себя наблюдение и выработку решений, необходимых для достижения бизнес-целей посредством защиты информационных активов. Управление ИБ выражается через формулирование и использование политик ИБ, процедур и рекомендаций, которые затем применяются повсеместно в организации всеми лицами, связанными с ней.

***Система управления***

Система управления использует совокупность ресурсов для достижения целей организации. Система управления организации включает в себя структуру, политики, планирование, обязательства, методы, процедуры, процессы и ресурсы.

*В части ИБ система управления позволяет организации:*

– удовлетворять требования безопасности клиентов и других заинтересованных лиц;

– улучшать планы и деятельность организации;

– соответствовать целям ИБ организации;

– выполнять нормативы, законодательство и отраслевые приказы;

– организованно управлять информационными активами для содействия постоянному улучшению и коррекции текущих целей организации.

**3.3. Процессный подход**

Организации нужно вести разные виды деятельности и управлять ими для того, чтобы функционировать эффективно и результативно. Любой вид деятельности, использующий ресурсы, нуждается в управлении для того, чтобы обеспечить возможность преобразования входов в выходы посредством совокупности взаимосвязанных действий, – это также называется процессом.

Выход одного процесса может непосредственно формировать вход следующего процесса, и обычно такая трансформация происходит в планируемых и управляемых условиях. Применение системы процессов в рамках организации вместе с идентификацией и взаимодействием этих процессов, а также их управлением может быть определено как «процессный подход».

***Дополнительная информация*** *(в стандарте отсутствует)*

Родоначальником процессного подхода к управлению качеством принято считать американского ученого Уолтера Шухарта. Его книга начинается с выделения 3-х стадий в *управлении качеством результатов деятельности организации:*

1) разработка спецификации (техническое задание, технические условия, критерии достижения целей) того, что требуется;

2) производство продукции, удовлетворяющей спецификации;

3) проверка (контроль) произведенной продукции для оценки ее соответствия спецификации.

Шухарт одним из первых предложил линейное восприятие указанных стадий замкнуть в цикл, который он отождествил с «динамическим процессом приобретения знаний».

После первого цикла результаты проверки должны являться основой совершенствования спецификации на продукцию. Далее производственный процесс корректируется на основе уточненной спецификации, а новый результат производственного процесса опять же подвергается проверке и т. д.

Американский ученый Эдвардс Деминг трансформировал цикл Шухарта в форму, наиболее часто встречаемую сегодня. Он, чтобы перейти от контроля качества к управлению качеством, дал более общие названия каждому из этапов, и, кроме того, добавил еще один, 4-й этап, с помощью которого он хотел обратить внимание американских менеджеров на то, что они недостаточно анализируют полученную на третьем этапе информацию и не улучшают процесс. Именно поэтому этот этап называется «воздействуй» (Act), и соответственно цикл Шухарта-Деминга называют моделью «PDCA» или «PDSA»:

– *Plan – Планирование* – идентификация и анализ проблем; оценка возможностей, постановка целей и разработка планов;

– *Do – Реализация* – поиск решения проблем и реализация планов;

– *Check (Study) – Оценка результативности* – оценка результатов реализации и выводы в соответствии с поставленной задачей;

– *Act – Улучшение* – принятие решений на основе полученных выводов, коррекция и улучшение работы.

***Модель «PDCA» для СУИБ***

*Планирование – Реализация – Контроль – Улучшение*

1. *Планирование (разработка и проектирование):* установление целей, политик, элементов управления, процессов и процедур СУИБ для достижения результатов, соответствующих общей политике и целям организации.

2. *Реализация (внедрение и обеспечение функционирования):* внедрение и применение политик ИБ, элементов управления, процессов и процедур СУИБ по оценке и обработке рисков и инцидентов ИБ.

3. *Контроль (мониторинг и анализ функционирования):* оценка результативности выполнения требований политик, целей ИБ и эффективности функционирования СУИБ и оповещение высшего руководства о результатах.

4. *Улучшение (сопровождение и усовершенствование):* проведение корректирующих и предупреждающих действий, основанных на результатах аудита и анализа со стороны руководства для достижения улучшения СУИБ

Метод и цикл Шухарта-Деминга, который чаще называют циклом Деминга, обычно иллюстрируют схему управления любым процессом деятельности. Он с необходимыми уточнениями к настоящему времени получил широкое применение в международных стандартах управления:

– качеством продукции ISO 9000;
– охраной окружающей среды ISO 14000;
– техникой безопасности и охраной труда OHSAS 18000;
– информационными сервисами ISO/IEC 20000;
– безопасностью пищевой продукции ISO 22000;
– информационной безопасностью ISO/IEC 27000;
– безопасностью ISO 28000;
– непрерывностью бизнеса ISO 22300;
– рисками ISO 31000;
– энергетикой ISO 50000.

**3.4. Важность СУИБ**

Организации следует определить риски, связанные с информационными активами. Достижение ИБ требует управления риском и охватывает риски физические, человеческие и технологические, относящиеся к угрозам, касающимся всех форм информации внутри организации или используемой организацией.

Принятие СУИБ является стратегическим решением для организации, и необходимо, чтобы это решение постоянно интегрировалось, оценивалось и обновлялось в соответствии с потребностями организации.

На разработку и реализацию СУИБ организации влияют потребности и цели организации, требования безопасности, используемые бизнес-процессы, а также размер и структура организации. Разработка и функционирование СУИБ должны отражать интересы и требования ИБ всех заинтересованных лиц организации, включая клиентов, поставщиков, бизнес-партнеров, акционеров и других третьих сторон.

Во взаимосвязанном мире информация и относящиеся к ней процессы, системы и сети составляют критичные активы. Организации и их ИС и сети сталкиваются с угрозами безопасности из широкого диапазона источников, включая компьютерное мошенничество, шпионаж, саботаж, вандализм, а также пожар и наводнение. Повреждения ИС и систем, вызванные вредоносным ПО, действиями хакеров и DoS-атаками, стали более распространенными, более масштабными и более изощренными.

СУИБ важна для предприятий как государственного, так приватного сектора. В любой отрасли СУИБ является необходимым инструментом для поддержания электронного бизнеса и важна для действий по управлению риском. Взаимосвязь общедоступных и приватных сетей и обмен информационными активами усложняют управления доступом к информации и ее обработку.

Кроме того, распространение мобильных устройств хранения данных, содержащих информационные активы, может ослабить эффективность традиционных мер защиты. Когда организации принимают семейство стандартов СУИБ, способность применения последова-

тельных и взаимоузнаваемых принципов ИБ можно продемонстрировать бизнес-партнерам и другим заинтересованным сторонам.

ИБ не всегда учитывается при создании и разработке ИС. Кроме того, часто считается, что ИБ – это техническая проблема. Однако ИБ, которая может быть достигнута с помощью технических средств, ограничена и может быть неэффективной, не будучи поддержанной соответствующим управлением и процедурами в контексте СУИБ. Встраивание системы безопасности в функционально завершенную ИС может быть сложным и дорогостоящим.

СУИБ включает в себя идентификацию имеющихся мер защиты и требует тщательного планирования и внимания к деталям. Например, меры разграничения доступа, которые могут быть техническими (логическими), физическими, административными (управленческими), или их комбинацией, гарантируют, что доступ к информационным активам санкционируется и ограничивается на основании требований бизнеса и ИБ.

*Успешное применение СУИБ важно для защиты информационных активов, поскольку позволяет:*

– повысить гарантии того, что информационные активы адекватно защищены на непрерывной основе от угроз ИБ;

– поддерживать структурированную и всестороннюю систему оценки угроз ИБ, выбора и применения соответствующих мер защиты, измерения и улучшения их эффективности;

– постоянно улучшать среду управления организации;

– эффективно соответствовать правовым и нормативным требованиям.

**3.5. Внедрение, контроль, сопровождение и улучшение СУИБ**

Внедрение, контроль, сопровождение и улучшение СУИБ являются оперативными этапами развития СУИБ.

*Оперативные этапы СУИБ определяют следующие составляющие:*

– общие положения;

– требования ИБ;

– решающие факторы успеха СУИБ.

*Оперативные этапы СУИБ обеспечивают следующие мероприятия:*

– оценка рисков ИБ;

– обработка рисков ИБ;

– выбор и внедрение мер защиты;

– контроль и сопровождение СУИБ;

– постоянное улучшение.

***Общие положения***

*Организация должна предпринимать следующие шаги по внедрению, контролю, сопровождению и улучшению ее СУИБ:*

– определение информационных активов и связанных с ними требований ИБ;

– оценка и обработка рисков ИБ;

– выбор и внедрение соответствующих мер защиты для управления неприемлемыми рисками;

– контроль, сопровождение и повышение эффективности мер защиты, связанных с информационными активами организации.

Для гарантии того, что СУИБ эффективно защищает информационные активы организации на постоянной основе, необходимо постоянно повторять все шаги, чтобы выявлять изменения рисков или стратегии организации или бизнес-целей.

***Требования ИБ***

*В пределах общей стратегии и бизнес-целей организации, ее размера и географического распространения требования ИБ могут быть определены в результате понимания:*

– информационных активов и их ценности;

– бизнес-потребностей в работе с информацией;

– правовых, нормативных и договорных требований.

*Проведение методической оценки рисков, связанных с информационными активами организации, включает в себя анализ:*

– угроз активам;

– уязвимостей активов;

– вероятности материализации угрозы;

– возможного влияния инцидента ИБ на активы.

Расходы на соответствующие меры защиты должны быть пропорциональны предполагаемому бизнес-влиянию от материализации риска.

***Оценка рисков ИБ***

Управление рисками ИБ требует соответствующего метода оценки и обработки риска, который может включать оценку затрат и преимуществ, правовых требований, проблем заинтересованных сторон, и других входных и переменных данных.

Оценки риска должны идентифицировать, измерить и установить приоритеты для рисков с учетом критерия принятия риска и целей организации. Результаты помогут выработать и принять соответствующие управленческие решения для действия и установления приоритетов по управлению рисками ИБ и внедрению мер защиты, выбранных для защиты от этих рисков.

Оценка риска должна включать систематический подход к оценке масштаба рисков (анализ риска) и процесс сравнения оцененных рисков с критерием риска для определения серьезности рисков (оценивание риска).

Оценки риска должны осуществляться периодически, чтобы вносить изменения в требования ИБ и ситуации риска, например, в активы, угрозы, уязвимости, влияния, оценивание риска, и в случае значительных изменений. Эти оценки риска должны осуществляться методично, чтобы обеспечить сопоставимые и воспроизводимые результаты.

Оценка риска ИБ должна четко определять сферу применения, чтобы быть эффективной, и содержать взаимодействия с оценками риска в других сферах, по возможности.

Стандарт ISO/IEC 27005 представляет руководство по управлению рисками ИБ, включая рекомендации по оценке, обработке, принятию, оповещению, мониторингу и анализу риска.

***Обработка рисков ИБ***

Перед рассмотрением обработки риска организации следует установить критерий для определения, можно принять риски или нет. Риски можно принять, если риск низкий или цена обработки не рентабельна для организации. Такие решения должны быть записаны.

Для каждого риска, определенного оценкой риска, следует принять решение о его обработке. *Возможные варианты обработки риска включают:*

– применение соответствующих мер защиты для снижения рисков;

– осознанное и объективное принятие рисков в строгом соответствии с политикой организации и критерием принятия риска;

– предотвращение рисков путем исключения действий, приводящих к появлению рисков;

– обмен связанными рисками с другими сторонами, например, страховщиками или поставщиками.

Соответствующие меры защиты от тех рисков, для которых принято решение об их применении с целью обработки рисков, дожны быть выбраны и внедрены.

***Выбор и внедрение мер защиты***

После определения требований к ИБ, определения и оценки рисков ИБ для информационных активов и принятия решений по обработке рисков ИБ должны быть выбраны и внедрены соответствующие меры защиты для снижения рисков.

*Меры и средства ИБ должны гарантировать снижение рисков до приемлемого уровня с учетом:*

– требований и ограничений национального и международного законодательства и нормативов;

– целей организации;

– операционных требований и ограничений;

– цены их внедрения и функционирования для снижения рисков, пропорциональной требованиям и ограничениям организации;

– их внедрения для контроля, оценки и улучшения результативности и эффективности мер и средств ИБ для поддержки целей организации;

– необходимости сбалансировать инвестиции на внедрение и функционирование мер защиты от вероятных потерь в результате инцидентов ИБ.

Меры защиты, изложенные в ISO/IEC 27002, общепризнаны как лучшие методы, применимые к большинству организаций и легко приспосабливаемые для организаций разной величины и структуры. Другие стандарты семейства стандартов СУИБ рекомендуют выбор и применение мер защиты, изложенных в стандарте ISO/IEC 27002, для СУИБ.

Меры и средства ИБ при разработке ИС следует рассматривать на стадии формирования системных и проектных требований и технического задания. Невыполнение этого может привести к дополнительным затратам и менее эффективным решениям и, может быть, в худшем случае, к невозможности достичь адекватной безопасности.

Меры защиты следует выбирать из стандарта ISO/IEC 27002 или других перечней, или создавать новые при особой необходимости. Следует осознавать, что некоторые меры защиты могут не подойти для каждой ИС или среды или быть неприемлемыми для всех организаций.

Иногда требуется время для внедрения набора мер защиты и в течение этого времени риск может быть выше приемлемого уровня долгое время. Критерий риска должен предусматривать приемлемость риска на короткое время, пока меры защиты внедряются. Заинтересованные стороны должны быть информированы об уровнях риска, которые оцениваются и прогнозируются в разные моменты времени, по мере последовательного внедрения средств защиты.

Надо понимать, что существующих мер защиты может быть недостаточно для достижения полноценной ИБ. Следует предпринять дополнительные управленческие действия для контроля, оценки и улучшения результативности и эффективности мер и средств ИБ для поддержки целей организации.

Выбор мер и средств ИБ должен быть задокументирован в Положении о применимости для соблюдения требований ИБ.

***Контроль и сопровождение СУИБ***

Организация должна контролировать и сопровождать СУИБ путем мониторинга и оценки деятельности на предмет соответствия политикам и целям организации и предоставления руководству результатов для анализа. Этот анализ СУИБ позволит наглядно показать, что СУИБ содержит специальные меры защиты, способные обрабатывать риски в сфере применения СУИБ. Кроме того, на основе записей этих контролируемых сфер СУИБ предоставляет данные проверки и корректирующих, профилактических и улучшающих действий.

***Постоянное улучшение***

Целью постоянного улучшения СУИБ является увеличение вероятностей достижения целей ИБ. Постоянное улучшение следует сфокусировать на поиске возможностей для улучшения и предоположении, что управленческая деятельность не так хороша, как могла бы быть.

*Действия по улучшению содержат следующее:*

– анализ и оценка существующей ситуации для определения сфер улучшения;

– формирование целей улучшения;

– поиск возможных решений для достижения целей;

– оценка этих решений и осуществление выбора;

– реализация выбранного решения;

– измерение, проверка, анализ и оценка результатов реализации для определения того, что цели достигнуты;

– формализованные изменения.

Результаты следует пересматривать, при необходимости, для определения дальнейших возможностей улучшения. В этом случае, улучшение является непрерывным действием, т.е. действия часто повторяются. Отзывы клиентов и других заинтересованных сторон, аудиты и анализ СУИБ могут также использоваться для определения возможностей улучшения.

**3.6. Решающие факторы успеха СУИБ**

Для успешной реализации СУИБ, позволяющей организации достичь своих бизнес-целей, имеет значение большое количество факторов. Примеры решающих факторов успеха включают в себя следующие:

– политика ИБ, цели и деятельность, ориентированная на цели;

– подход и структура для разработки, внедрения, контроля, сопровождения и улучшения ИБ, соответствующие корпоративной культуре;

– видимая поддержка и обязательства со стороны всех уровней управления, особенно высшего руководства:

– понимание требований защиты информационных активов, достигаемое применением управления рисками ИБ (см. ISO/IEC 27005);

– эффективное информирование, обучение и образовательная программа по ИБ, доводящая до сведения всех сотрудников и других причастных сторон их обязательства по ИБ, сформулированные в политиках ИБ, стандартах и т. д., а также их мотивирование к соответствующим действиям;

– эффективный процесс управления инцидентами ИБ:

– эффективный подход к управлению непрерывностью бизнеса;

– система измерения, используемая для оценки управления ИБ, и предложения по улучшению, взятые из отзывов.

СУИБ увеличивает вероятность того, что организация будет последовательно достигать решающих факторов успеха, необходимых для защиты ее информационных активов.

**3.7. Преимущества внедрения стандартов семейства СУИБ**

Преимущества реализации СУИБ проистекают, прежде всего, из сокращения рисков ИБ (т.е. снижения вероятности инцидентов ИБ и/или вызванного ими влияния). В частности, преимущества, полученные от принятия семейства стандартов СУИБ, содержат:

– структурированную базу для поддержания процесса определения, внедрения, функционирования и сопровождения комплексной, рентабельной, значимой, интегрированной и ориентированной СУИБ для удовлетворения разных потребностей организации;

– помощь руководству для стабильного управляющего и операционного подхода к управлению ИБ ответственным образом в контексте государственного и корпоративного управления рисками, включая обучение и тренинг владельцев систем и бизнеса по комплексному управлению ИБ;

– продвижение общепринятых лучших методов ИБ в необязывающей форме, предоставляющей организациям свободу принятия и улучшения мер защиты, соответствующих их особенностям и поддерживающих в случаях внутренних и внешних изменений;

– предоставление общего языка и концептуальной базы для ИБ, что облегчает взаимопонимание бизнес-партнеров с похожими СУИБ, особенно, если они требуют сертификат соответствия ISO/IEC 27001 от аккредитованного органа сертификации;

– повышение доверия заинтересованных сторон к организации;

– удовлетворение социальных нужд и ожиданий;

– более эффективное экономическое управление инвестициями в ИБ.

На этом рассмотрение стандарта ISO/IEC 27000 заканчиваем.

**Сертификация СУИБ**

Для подтверждения соответствия существующей в организации СУИБ требованиям стандарта, а также ее адекватности существующим бизнес рискам необходима процедура добровольной сертификации. Хотя без этого можно и обойтись, в большинстве случаев сертификация полностью оправдывает вложенные средства и время.

Во-первых, официальная регистрация СУИБ организации в реестре авторитетных органов, таких как служба аккредитации Великобритании (*UKAS*), укрепляет репутацию фирмы, повышает интерес со стороны потенциальных клиентов, инвесторов и кредиторов.

Во-вторых, в результате успешной сертификации расширяется сфера деятельности компании за счет получения возможности участия в тендерах и развития бизнеса на международном уровне. В наиболее чувствительных к уровню ИБ областях, такой, например, как финансы, наличие сертификата соответствия ISO/IEC 27001 начинает выступать как обязательное требование для осуществления деятельности.

Также очень важно, что процедура сертификации оказывает серьезное мотивирующее и мобилизующее воздействие на персонал компании: повышается уровень осведомленности сотрудников, эффективнее выявляются и устраняются недостатки и несоответствия в СУИБ, что в перспективе означает для организации снижение среднестатистического ущерба от инцидентов ИБ, а также сокращение накладных расходов на эксплуатацию информационных систем. Вполне возможно, наличие сертификата позволит застраховать информационные риски организации на более выгодных условиях.

Следует подчеркнуть, что все перечисленные преимущества организация получает только в том случае, если речь идет о системе сертификации, имеющей международное признание, в рамках которой обеспечивается надлежащее качество проведения работ и достоверность результатов.

***Подготовка к сертификации***

Подготовка организации к сертификации по ISO/IEC 27001 – процесс довольно длительный и трудоемкий. В общем случае, он включает в себя 6 последовательных этапов, которые выполняются организацией, как правило, при помощи внешних консультантов.

1. Предварительный аудит СУИБ, в ходе которого оценивается текущее состояние, осуществляется инвентаризация и документирование всех основных составляющих СУИБ, определяются область и границы сертификации и выполняется еще целый ряд необходимых подготовительных действий. По результатам аудита разрабатывается детальный план мероприятий по подготовке к сертификации.

2. Оценка информационных рисков, основной целью которой является определение применимости описанных в стандарте механизмов контроля в данной конкретной организации, подготовка декларации о применимости и плана обработки рисков.

3. Анализ расхождений с требованиями стандарта, в результате которого оценивается текущее состояние механизмов контроля в организации и идентифицируются расхождения с декларацией о применимости.

4. Планирование и подготовка программы внедрения недостающих механизмов контроля, по каждому из которых разрабатывается соответствующая стратегия и план.

5. Работы по внедрению недостающих механизмов контроля, которые включают в себя 3 основные составляющие:

– подготовка и повышение осведомленности сотрудников (обучение и тренинги);

– подготовка документации СУИБ (политики, стандарты, процедуры, регламенты, инструкции, планы);

– подготовка свидетельств функционирования СУИБ (отчеты, протоколы, приказы, записи, журналы событий и т.п).

6. Подготовка к сертификационному аудиту: анализируется состояние СУИБ, оценивается степень ее готовности к сертификации, уточняется область и границы сертификации, проводятся соответствующие переговоры с аудиторами органа по сертификации.

***Точки преткновения***

В процессе внедрения СУИБ возникает много точек преткновения. Часть из них связаны с нарушением описанных выше фундаментальных принципов управления безопасностью. Серьезные затруднения для украинских организаций лежат в законодательной области.

Использование ISO/IEC 27001—2005 как национального стандарта, в то время как уже введен в действие ISO/IEC 27001—2013, а также неотрегулированность системы сертификации средств защиты информации серьезно затрудняет выполнение одного из главных требований стандарта – соответствие действующему законодательству.

Источником затруднений нередко служит неправильное определение области действия и границ СУИБ. Слишком широкая трактовка области действия СУИБ, например, включение в эту область всех бизнес-процессов организации, значительно снижает вероятность успешного завершения проекта по внедрению и сертификации СУИБ.

Столь же важно правильно представлять, где проходят границы СУИБ и каким образом она связана с другими системами управления и процессами организации. Например, СУИБ и система управления непрерывностью бизнеса (СУНБ) организации тесно пересекаются. Последняя является одной из 14 определяемых стандартом областей контроля ИБ. Однако СУИБ включает в себя только ту часть СУНБ, которая связана с ИБ – это защита критичных бизнес процессов организации от крупных сбоев и аварий информационных систем. Другие аспекты СУНБ выходят за рамки СУИБ.

***Стандарт – гарантия безопасности***

Сегодня организация работы серьезной и эффективной компании, претендующей на успешное развитие, обязательно базируется на современных информационных технологиях. Поэтому обратить внимание на стандарты управления ИБ стоит компаниям любого масштаба. Как правило, вопросы управления ИБ тем актуальнее, чем крупнее компания, чем шире масштаб ее деятельности и претензии на развитие, и, как следствие, выше ее зависимость от информационных технологий.

Использование семейства международных стандартов ISO/IEC 27k позволяет существенно упростить создание, эксплуатацию и развитие СУИБ. Требования нормативной базы и рыночные условия вынуждают организации применять международные стандарты при разработке планов и политик обеспечения ИБ и демонстрировать свою приверженность путем проведения аудитов и сертификаций ИБ. Соответствие требованиям стандарта представляет определенные гарантии наличия в организации базового уровня ИБ, что оказывает положительное влияние на имидж компании.

# 2. Требования к суиб (стандарт ISO/IEC 27001:2013)

В 1998 году появилась вторая часть британского национального стандарта – BS 7799—2 «СУИБ. Спецификация и руководство по применению», в 2002 году она была пересмотрена, а в конце 2005 года была принята в качестве международного стандарта ISO/IEC 27001 «ИТ. Методы защиты. СУИБ. Требования». 25 сентября 2013 года состоялось последнее обновление стандарта.

*Стандарт состоит из следующих разделов:*

Предисловие
0. Введение
1. Сфера применения
2. Нормативные ссылки
3. Термины и определения
4. Контекст организации
5. Лидерство
6. Планирование
7. Поддержка
8. Эксплуатация
9. Оценка результативности
10. Улучшение

*Этапам модели «PDCA» соответствуют следующие разделы стандарта:*

– планирование;
– эксплуатация;
– оценка результативности;
– улучшение.

Стандарт был подготовлен для реализации требований по созданию, внедрению, сопровождению и постоянному улучшению СУИБ. Принятие СУИБ является стратегическим решением для организации. Разработка и внедрение СУИБ организации зависит от потребностей и целей организации, требований по безопасности, существующих процессов организации, размера и структуры организации. Все эти факторы влияния, как известно, со временем меняются.

СУИБ обеспечивает конфиденциальность, целостность и доступность информации за счет применения процесса управления рисками и придает уверенность заинтересованным сторонам в том, что риски адекватно управляются.

Важно, чтобы СУИБ являлась частью и была интегрирована с процессами организации и общей структурой управления, а также ИБ была применена при разработке процессов, ИС и элементов управления. Как правило, внедрение СУИБ масштабируется в соответствии с потребностями организации.

# 1. Сфера применения

Стандарт устанавливает в контексте организации требования к созданию, внедрению, сопровождению и постоянному улучшению СУИБ. Стандарт также включает требования по оценке и обработке рисков ИБ в соответствии с потребностями организации. Требования, изложенные в стандарте, носят общий характер и предназначены для применения всеми организациями, независимо от типа, размера или характера. Исключение любого из требований, указанных в следующих разделах, не является приемлемым, если организация заявляет о соответствии стандарту.

# Конец ознакомительного фрагмента.