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.

Разделы «2.Нормативные ссылки» и «3.Термины и определения» пропускаем.

4. Контекст организации

Организация должна определить внешние и внутренние аспекты, которые имеют отношение к ее цели и влияют на ее способность к достижению ожидаемых результатов от СУИБ.

Организация должна определить:

– заинтересованные стороны, имеющие отношение к СУИБ;

– требования этих заинтересованных сторон, имеющих отношение к ИБ.

Организация для определения сферы применения СУИБ должна определить границы и возможность применения СУИБ.

При определении сферы применения СУИБ организация должна рассмотреть вопросы, упомянутые выше:

– внешние и внутренние аспекты;

– требования заинтересованных сторон;

– взаимосвязи и зависимости между деятельностью, выполняемой организацией, и деятельностью, выполняемой другими организациями.

Сфера применения должна быть доступна в виде документированной информации.

5. Лидерство

Лидерство и обязательства

Высшее руководство должно продемонстрировать лидерство и обязательства в отношении СУИБ путем:

– обеспечения политики ИБ и целей ИБ, которые разработаны и совместимы со стратегическими задачами организации;

– обеспечения интеграции требований СУИБ в процессы организации;

– обеспечения того, чтобы ресурсы, необходимые для системы менеджмента информационной безопасности, были доступны;

– информирования о важности достижения результативности УИБ и о соответствии требованиям СУИБ;

– обеспечения того, что СУИБ позволяет достигать желаемых результатов;

– поддержки и управления персоналом, способствующим эффективности СУИБ;

– содействия постоянному улучшению;

– поддержки других соответствующих управленческих ролей для демонстрации их лидерства, насколько это применимо к сфере их ответственности.

Политика

Высшее руководство должно разработать соответствующую целям организации политику ИБ, которая должна:

– соответствовать целям ИБ;

– содержать цели ИБ или обеспечивать основу для достижения целей ИБ;

– включать обязательства по соблюдению требований ИБ;

– включать обязательства по постоянному улучшению СУИБ.

Политика ИБ должна быть:

– доведена до персонала организации;

– доступна как документированная информация;

– доступна всем заинтересованным сторонам.

Организационные роли, обязанности и полномочия

Высшее руководство должно быть уверенным, что обязанности и полномочия ролей, относящихся к ИБ, обозначены и сообщены.

Высшее руководство должно обозначить обязанности и полномочия для:

– обеспечения соответствия СУИБ требованиям этого стандарта;

– оповещения высшего руководства о результативности СУИБ.

6. Планирование (1-й этап «PDCA»)

Этап планирования СУИБ обеспечивают следующие мероприятия:

– определение целей ИБ и мер по их достижению;

– действия по обработке рисков и возможностей.

Определение целей ИБ и мер по их достижению

Организация должна установить цели ИБ для соответствующих функций и на соответствующих уровнях.

Цели ИБ должны:

– соответствовать политике ИБ;

– быть измеримыми (если это возможно);

– принимать во внимание действующие требования ИБ, результаты оценки и обработки рисков;

– быть известны соответствующему персоналу организации;

– обновляться по мере необходимости.

Организация должна сохранять документированную информацию о целях ИБ.

При планировании мер по достижению целей ИБ организация должна определить:

– что будет сделано;

– какие ресурсы потребуются;

– кто будет нести ответственность;

– когда меры будут реализованы;

– как будут оцениваться результаты.

Действия по обработке рисков и возможностей

При планировании СУИБ организация должна учитывать аспекты и требования, указанные в контексте организации, и определить риски и возможности, которые должны быть направлены на:

– обеспечение того, чтобы СУИБ позволило достигать желаемых результатов;

– предотвращение или уменьшение нежелательных эффектов;

– обеспечение непрерывного совершенствования.

Организация должна планировать:

– процессы оценки и обработки рисков;

– действия по осуществлению и интеграции работ в процессах СУИБ и оценке их результативности.

Оценка рисков ИБ

Организация должна определить и внедрить процесс оценки рисков ИБ, состоящий из разработки критериев, определения, анализа рисков и сравнения его результатов с критериями для рисков ИБ.

На основании процесса оценки рисков ИБ организации следует:

– установить и поддерживать критерии для рисков ИБ, которые состоят из критериев для проведения оценки и принятия рисков ИБ;

– определить риски ИБ:

• применить процесс оценки рисков ИБ для выявления рисков, связанных с потерей конфиденциальности, целостности и доступности информации в рамках СУИБ (§);

• определить владельцев рисков;

– проанализировать риски ИБ:

• определить реалистичную вероятность возникновения рисков §;

• определить потенциальные последствия, которые могут возникнуть в случае возникновения рисков §;

• определить уровни риска;

– оценить риски ИБ:

• сравнить результаты анализа рисков с установленными критериями для рисков;

• установить приоритеты по обработке рисков для проанализированных рисков;

– гарантировать, что повторная оценка рисков ИБ позволит получить логичные, обоснованные и сопоставимые результаты.

Организация должна сохранять документированную информацию о процессе оценки рисков ИБ.

Обработка рисков ИБ

Организация должна определить и внедрить процесс обработки рисков ИБ, состоящий из выбора варианта обработки, его реализации и принятия остаточных рисков ИБ.

На основании процесса обработки рисков ИБ организации следует:

– выбрать подходящий вариант обработки рисков ИБ, принимая во внимание результаты оценки рисков;

– определить все элементы управления, которые необходимы для реализации выбранного варианта обработки рисков ИБ;

– сравнить определенные элементы управления с теми, которые приведены в Приложении А и убедиться в том, что не были упущены необходимые элементы;

– разработать Положение о Применимости (англ. Statement of Applicability, SoA), которое содержит необходимые элементы управления и обоснования их включения (независимо от того, реализованы они или нет), а также обоснования исключений элементов управления из Приложения А;

– сформулировать план по обработке рисков ИБ;

– согласовать с владельцами рисков план по обработке рисков ИБ и получить (от владельцев рисков) согласие на принятие остаточных рисков ИБ.

Организация должна сохранять документированную информацию о процессе обработки рисков ИБ.

7. Поддержка

Поддержка СУИБ определяется следующими составляющими:

– ресурсы;

– компетенции;

– осведомленность;

– коммуникации;

– документированная информация.

Ресурсы

Организация должна определить и предоставить ресурсы, необходимые для разработки, внедрения, сопровождения и постоянного улучшения СУИБ.

Компетенции

Организация должна:

– определять необходимую компетентность персонала, который самостоятельно выполняет работу, что влияет на результативность ИБ;

– обеспечить то, что этот персонал обладает необходимыми компетенциями на основе соответствующего обучения, тренингов или опыта;

– при необходимости принять меры для получения необходимых компетенций и оценить эффективность принятых мер;

– сохранять соответствующую документированную информацию в качестве доказательств наличия компетенций.

Соответствующие меры могут включать, например, проведение тренинга, наставничество или переаттестацию действующих сотрудников; или наем / привлечение по контракту компетентных лиц.

Осведомленность

Персонал, выполняющий работы в рамках организации, должен быть осведомлен:

– о политике ИБ;

– о вкладе в повышение результативности СУИБ, включая выгоды от улучшения состояния ИБ;

– о последствиях в результате не выполнения требований СУИБ.

Коммуникации

Организация должна определить необходимые внутренние и внешние коммуникации, относящиеся к СУИБ, включая:

– о чем сообщать;

– когда сообщать;

– кому сообщать;

– кто должен участвовать в коммуникациях;

– процессы осуществления коммуникаций.

Документированная информация

СУИБ организации должна включать документированную информацию:

– требуемую настоящим стандартом;

– определенную организацией в качестве необходимой для обеспечения результативности СУИБ.

Степень (детализация) документированной информации для СУИБ одной организации может отличаться от другой в зависимости от:

– размера организации и ее вида деятельности, процессов, продуктов и услуг;

– сложности процессов и их взаимодействия;

– компетенции персонала.

При создании и обновлении документированной информации организация должна обеспечить соответствующее:

– идентификацию и описание (например: название, дата, автор или ссылка);

– оформление (например: язык, версия ПО, рисунки) и тип носителя (например: электронный, бумажный);

– рассмотрение и утверждение на предмет пригодности для применения и адекватности.

Документированная информация СУИБ должна управляться для обеспечения:

– доступности и пригодности для использования;

– адекватной защиты (например: от потери конфиденциальности, неправильного использования или потери целостности).

Для управления документированной информацией организация должна рассмотреть следующие мероприятия (где применимо):

– распространение информации, доступ, восстановление и использование;

– хранение и сохранность, в том числе сохранение удобочитаемости;

– контроль изменений (например, управление версиями);

– архивирование и уничтожение.

Документированная информация внешнего происхождения, определенная организацией в качестве необходимой для планирования и функционирования СУИБ, должна соответствующим образом определяться и управляться.

Доступ предполагает принятия решения о доступе только на просмотр документированной информации или предоставлении полномочий для просмотра и внесения изменений в документированной информации и т. д.

8. Эксплуатация (2-й этап «PDCA»)

Этап эксплуатации СУИБ обеспечивают следующие мероприятия:

– оперативное планирование и контроль;

– оценка рисков ИБ;

– обработка рисков ИБ.

Оперативное планирование и контроль

Организация должна планировать, внедрять и контролировать процессы, необходимые для выполнения требований ИБ и реализации действий по обработке рисков и возможностей. Организация также должна выполнять планы по достижению целей ИБ.

Организация должна сохранять документированную информацию в объеме, необходимом для получения уверенности в том, что процессы осуществляются так, как запланировано.

Организация должна управлять планируемыми изменениями и рассматривать последствия случайных изменений, принимать меры по смягчению неблагоприятных последствий при необходимости.

Организация должна обеспечить, что переданные на аутсорсинг процессы определены и управляются.

Оценка рисков ИБ

Организация должна выполнять оценку рисков ИБ через запланированные интервалы времени, либо в случае предполагающихся или уже происходящих существенных изменений, с учетом установленных критериев.

Организация должна сохранять документированную информацию о результатах оценки рисков ИБ.

Обработка рисков ИБ

Организация должна реализовать план обработки рисков ИБ. Организация должна сохранять документированную информацию о результатах обработки рисков ИБ.

9. Оценка результативности (3-й этап «PDCA»)

Этап оценки результативности СУИБ обеспечивают следующие мероприятия:

– мониторинг, измерение, анализ и оценка;

– внутренний аудит;

– анализ со стороны руководства.

Мониторинг, измерение, анализ и оценка

Организация должна оценивать состояние ИБ и результативность СУИБ.

Организация должна определить:

– что необходимо отслеживать и измерять, в том числе процессы ИБ и элементы управления;

– методы мониторинга, измерения, анализа и оценки, в зависимости от обстоятельств, в целях обеспечения достоверных результатов;

– когда должны проводиться действия по мониторингу и измерениям;

– кто должен осуществлять мониторинг и измерения;

– когда результаты мониторинга и измерений должны быть проанализированы и оценены;

– кто должен анализировать и оценивать эти результаты.

Организация должна сохранять соответствующую документированную информацию в качестве подтверждения результатов мониторинга и измерений.

Внутренний аудит

Организация должна проводить внутренние аудиты через запланированные промежутки времени для получения информации о состоянии СУИБ:

– на предмет соответствия собственным требованиям организации для своей СУИБ и требованиям настоящего стандарта;

– с целью оценки результативности внедрения и поддержки.

Перед проведением аудита организация должна определить программу, критерии и сферу применения для каждого аудита, а также аудиторов.

Программа аудита должна включать методы, распределение ответственности, требования к планированию и отчетности и учитывать важность процессов и результаты предыдущих аудитов.

Организация должна обеспечить:

– объективность и беспристрастность процесса аудита;

– направление результатов аудитов руководству соответствующего уровня;

– хранение документированной информации как свидетельства о программе аудита и результатах аудита.

Анализ со стороны руководства

Высшее руководство должно анализировать СУИБ организации через запланированные интервалы времени для обеспечения ее постоянной пригодности, адекватности и результативности.

Анализ со стороны руководства должен включать следующее:

– статус действий по результатам предыдущих анализов со стороны руководства;

– изменения внешних и внутренних аспектов, которые имеют отношение к СУИБ;

– обратную связь о состоянии ИБ, включая:

• несоответствия и корректирующие действия;

• результаты мониторинга и измерений;

• результаты аудита;

• результат достижения целей ИБ;

– обратную связь от заинтересованных сторон;

– результаты оценки рисков и статус выполнения плана по обработке рисков;

– возможности для постоянного улучшения.

Выводы анализа со стороны руководства должны включать решения, связанные с реализацией возможностей постоянного улучшения, и любые необходимые изменения в СУИБ.

Организация должна сохранять документированную информацию в качестве свидетельства о результатах анализа со стороны руководства.

10. Улучшение (4-й этап «PDCA»)

Этап улучшения СУИБ обеспечивают следующие мероприятия:

– корректирующие действия;

– постоянное улучшение.

Корректирующие действия

При появлении несоответствия организация должна:

– реагировать на несоответствие и в зависимости от обстоятельств принять меры по его управлению и исправлению или проработать последствие;

– оценить необходимость принятия действий для устранения причин несоответствия с целью предотвращения его повторения или появления в другом месте, для этого:

• изучить несоответствие;

• определить причину несоответствия;

• определить, существуют ли подобные несоответствия или потенциальные возможности их возникновения;

– реализовать любые необходимые корректирующие действия;

– проанализировать результативность выполненных корректирующих действий;

– при необходимости внести изменения в СУИБ.

Корректирующие действия должны быть адекватными последствиям выявленных несоответствий. Организация должна сохранять документированную информацию как свидетельства о:

– характере несоответствий;

– любых корректирующих действиях;

– результатах корректирующих действий.

Постоянное улучшение

Организация должна постоянно улучшать пригодность, адекватность и результативность СУИБ.

3. Свод правил управления ИБ (стандарт ISO/IEC 27002:2013)

В 2000 году первая часть британского национального стандарта BS 7799—1 «Практические правила управления ИБ» была принята в качестве международного стандарта ISO/IEC 17799 «ИТ. Практические правила управления ИБ». В 2005 году на его основе был разработан новый международный стандарт ISO/IEC 27002 «ИТ. Методы защиты. Свод норм и правил управления ИБ», который был опубликован в июле 2007 года. Последнее обновление стандарта состоялось 25 сентября 2013 года.

Стандарт предлагает рекомендации и основные принципы введения, реализации, поддержки и улучшения СУИБ в организации. Он может служить практическим руководством по разработке стандартов безопасности организации, для эффективной практики УИБ организаций и способствует укреплению доверия в отношениях между организациями.

Стандарт состоит из 14 разделов, посвященных мерам безопасности, которые все вместе содержат, в целом, 34 основные категории безопасности и 114 мер защиты:

1) политика ИБ (1);
2) организация ИБ (2);
3) безопасность, связанная с персоналом (3):
4) управление активами (3);
5) управление доступом (4);
6) криптография (1);
7) физическая и экологическая безопасность (2);
8) безопасность операций (7);
9) безопасность связи (2);
10) приобретение, разработка и поддержка ИС (3);
11) взаимоотношения с поставщиками (2);
12) управление инцидентами ИБ (1);
13) аспекты ИБ при управлении непрерывностью бизнеса (2);
14) соответствие требованиям (2).

Каждая основная категория безопасности включает в себя:

– цель ИБ;
– меры достижения этой цели.

Описание мер ИБ структурируется таким образом:

– меры и средства ИБ;
– рекомендации по их реализации.

1. Политика ИБ

1.1. Руководящие положения для ИБ

Цель: Реализовать требования политики ИБ и обеспечить поддержку для ИБ в соответствии с требованиями бизнеса и действующим законодательством.

Политика ИБ предполагает следующие мероприятия:

– документирование;

– пересмотр.

Документирование

Меры и средства

Политика ИБ документируется оформлением, утверждением, публикованием и доведением до персонала и внешних заинтересованных сторон.

Рекомендации по реализации

В лучшем случае, политика ИБ должна устанавливать ответственность руководства, а также излагать подход организации к УИБ.

Политика ИБ должна содержать требования:

– стратегии бизнеса;

– законодательства и договорных обязательств;

– защиты от существующих и потенциальных угроз ИБ.

Политика ИБ должна содержать положения по:

– определению ИБ, ее целей и принципов для руководства действиями по обеспечению ИБ;

– определению ответственности разных ролей с учетом специфики управления ИБ;

– изложения намерений руководства, поддерживающих цели и принципы ИБ в соответствии со стратегией и целями бизнеса;

– процессов управления изменениями и исключениями.

В худшем случае, политика ИБ должна поддерживаться специализированными политиками, направленными на внедрение управления ИБ и созданными специально для целевых групп внутри организации или выполнения конкретных задач.

Примерами таких задач могут быть:

– управление доступом;

– классификация активов;

– физическая и экологическая безопасность;

– следующие требования к пользователям:

• использование активов;

• чистый стол и чистый экран;

• политика коммуникаций;

• мобильные устройства и удалённая работа;

• ограничения на установку ПО;

– передача информации;

– защита от вредоносного ПО;

– управление техническими уязвимостями;

– управление средствами криптографии;

– безопасность коммуникаций;

– защита персональных данных;

– взаимоотношения с поставщиками.

Эти политики должна быть доведены до сведения персонала в рамках всей организации и сторонних организаций в актуальной, доступной и понятной форме путем проведения инструктажей и тренингов.

Если какие-либо политики ИБ должны применяться за пределами организации, в них не должна содержаться конфиденциальная информация.

В качестве названий политик ИБ могут использоваться такие термины, как стандарт, руководство или правила.

Пересмотр

Меры и средства

Политика ИБ должны быть пересмотрены через запланированные промежутки времени или в случае изменений с целью обеспечения ее постоянной пригодности, адекватности и эффективности.

Рекомендации по реализации

Политика ИБ должна иметь владельца, который утвержден руководством в качестве ответственного за разработку, пересмотр и оценку. Пересмотр заключается в оценке возможностей по улучшению политики ИБ организации и подхода к УИБ в ответ на изменения организационной среды, обстоятельств бизнеса, правовых условий или технической среды.

При пересмотре политики ИБ следует учитывать результаты пересмотров методов управления, для чего должны существовать определенные процедуры, в том числе график или период пересмотра.

2. Организация ИБ

Организацию ИБ определяют следующие составляющие:

– внутренняя организация;

– мобильные устройства и удалённая работа.

2.1. Внутренняя организация

Цель: Создать структуру управления для инициирования и управления внедрением и обеспечением ИБ в организации.

Внутренняя организация сферы ИБ предполагает следующие мероприятия:

– определение ответственности;

– разделение обязанностей;

– контакт с властями;

– контакт со специальными группами.

Определение ответственности

Меры и средства

Все ответственности в поле ИБ должны быть определены и закреплены.

Рекомендации по реализации

Закрепление ответственности должно соответствовать политике ИБ. Ответственности за защиту индивидуальных активов и осуществления процессов ИБ должны быть определены. Ответственности за действия по управлению рисками ИБ и, в частности, принятие остаточного риска должны быть определены. Эти ответственности должны быть дополнительно детализированы, при необходимости, для специфических мест и средств обработки информации.

Ответственные лица могут делегировать некоторые задачи безопасности другим. Впрочем они все равно несут за это ответственность, поэтому должны обеспечить правильное оформление такого делегирования.

Сферы ответственности должны быть зафиксированы.

В частности, необходимо учесть следующее:

– активы и процессы ИБ должны быть идентифицированы и определены;

– личная ответственность за каждый актив и процесс ИБ должна быть обозначена и ее детали задокументированы;

– уровни авторизации должны быть определены и задокументированы;

– назначенные быть ответственными в сфере ИБ должны быть компетентными и в курсе всех событий в этой сфере;

– координация и контроль аспектов ИБ взаимотношений с поставщиками должны быть идентифицированы и задокументированы.

Многие организации назначают отдельного менеджера по ИБ, возлагая на него всю ответственность за разработку и внедрение ИБ и поддержку актуальности мер и средств ИБ. Одной из распространенных практик является назначение владельца каждого актива, отвечающего за его безопасность.

Разделение обязанностей

Меры и средства

Противоречивые обязанности и зоны ответственности должны быть разделены для снижения возможностей несанкционированного изменения или неправильного использования активов организации.

Рекомендации по реализации

Следует четко обозначить, что никто не может получить доступ к использованию и модификации активов без идентификации и аутентификации. Инициация события должна быть

отделена от его авторизации. Возможность сговора должна быть учтена при выборе мер защиты.

В маленьких организациях сложно обеспечить разделение обязанностей, но принцип разделения должен быть применен настолько, насколько это возможно.

Разделение обязанностей является методом снижения риска случайного или преднамеренного нанесения вреда активам организации.

Контакт с властями

Меры и средства

Необходимые контакты с органами власти должны поддерживаться.

Рекомендации по реализации

В организациях должны применяться процедуры, определяющие, когда и с какими инстанциями (например правоохранительными, пожарными и надзорными органами) необходимо вступить в контакт, и каким образом следует своевременно сообщать о выявленных инцидентах ИБ, если есть подозрение о возможности нарушения закона.

Организациям, подвергающимся атаке через Интернет, может потребоваться привлечение сторонней организации (например интернет-провайдера или оператора телекоммуникаций) для принятия мер защиты от атаки.

Контакт со специальными группами

Меры и средства

Должны поддерживаться надлежащие контакты со специальными группами или форумами специалистов в области ИБ, а также профессиональными ассоциациями.

Рекомендации по реализации

Членство в группах или форумах следует рассматривать как средство для:

– повышения знания о «передовом опыте» и достижений ИБ на современном уровне;

– обеспечения уверенности в том, что понимание проблем ИБ является современным и полным;

– получения раннего оповещения в виде предупреждений, информационных сообщений и патчей[1], касающихся атак и уязвимостей;

– возможности получения консультаций специалистов по вопросам ИБ;

– совместного использования и обмена информацией о новых технологиях, продуктах, угрозах или уязвимостях;

– организация подходящих связей для обеспечения обработки инцидентов ИБ.

Соглашения об информационном обмене должны обеспечить улучшение кооперации и координации действий в сфере безопасности. Эти соглашения должны определить требования по защите конфиденциальной информации.

[1] Патч – блок изменений для оперативного исправления или нейтрализации ошибки в исполняемой программе. чаще всего поставляемый (или размещаемый на сайте разработчика) в виде небольшой программы, вставляющей исправления в объектный код соответствующих модулей приложения.

ИБ при управлении проектом

Меры и средства

ИБ должна обеспечиваться при управлении проектом, независимо от его типа.

Рекомендации по реализации

ИБ должна быть интегрирована|интегрированной, комплексной| в метод управления проектом|структуры|, чтобы гарантировать, что|который| риски|рисковый| ИБ идентифицированы|опознает| и являются частью проекта. Это относится к любому проекту, независимо от его содержания.

Метод управления проектом при использовании должен требовать, чтобы|который|:

– цели|задача| ИБ входили в проектные цели|задачу|;

– оценка риска|рисковый| ИБ проводилась|ведет| на ранней стадии проекта, чтобы идентифицировать|опознать| необходимые меры защиты|контроль, управляет|;

– ИБ была частью всех фаз|стадии| используемой проектной методологии.

Требования|импликацию| ИБ должны обеспечиваться и пересматриваться регулярно во всех проектах. Ответственность за ИБ нужно определить и применить к ролям, определенным методами управления проектом.

2.2. Мобильные устройства и удалённая работа

Цель: обеспечить безопасность удалённой работы и использования мобильных устройств.

Этот раздел рассматривает обеспечение ИБ при использовании:

– мобильных устройств;

– удалённой работы.

Мобильные устройства

Меры и средства

Политика и меры безопасности должны обеспечить управление рисками, связанными с использованием мобильных устройств.

Рекомендации по реализации

При использовании мобильных устройств необходимо уделить внимание тому, чтобы не скомпрометировать бизнес-информацию. Политика мобильных устройств должна учитывать риски работы с мобильными устройствами в незащищенной среде.

Политика мобильных устройств должна рассматривать:

– регистрацию мобильных устройств;

– требования физической защиты;

– ограничения на установку ПО;

– требования к версиям ПО мобильных устройств и применению патчей;

– ограничения на подключение к информационным сервисам;

– управление доступом;

– криптографические средства;

– защита от вредоносного ПО;

– дистанционное выключение, удаление или блокировку;

– резервное копирование;

– использование веб-сервисов и веб-приложений.

Следует проявлять осторожность при использовании мобильных устройств в общедоступных местах, конференц-залах и других незащищенных местах. Необходимо обеспечить защиту от несанкционированного доступа или раскрытия информации, хранимой и обрабатываемой этими устройствами, например с помощью средств криптографии.

Мобильные устройства необходимо также физически защищать от краж, особенно когда их оставляют в автомобилях или других видах транспорта, гостиничных номерах, конференц-залах и местах встреч. Для случаев потери или кражи мобильных устройств должна быть установлена специальная процедура, учитывающая законодательные, страховые и другие требования безопасности организации.

Устройства, в котором переносится важная, чувствительная или критическая информация бизнеса, не следует оставлять без присмотра и, по возможности, для обеспечения безопасности устройства должны быть физически заблокированы или использованы специальные замки.

Необходимо провести обучение сотрудников, использующих мобильные устройства, с целью повышения осведомленности о дополнительных рисках, связанных с таким способом работы, и мерах защиты, которые должны быть выполнены.

Там, где политика мобильных устройств разрешает использование личных мобильных устройств, политика и связанные с ней меры безопасности должны предусмотреть:

– разделение личного и делового использования устройств с применением ПО, которое поддерживает разделение и защищает бизнес-данные на личном устройстве;

– предоставление доступа пользователей к бизнес-информации только после заключения трудового договора, определяющего их обязанности (физическая защита, обновление ПО и т.д.), отказ в собственности на бизнес-данные, разрешение на удаленное уничтожение организацией данных в случае кражи или потери устройства или после завершения срока использования сервиса. Эта политика разрабатывается с учетом законодательства о конфиденциальности.

Беспроводная коммуникация мобильных устройств похожа на другие типы сетевой коммуникации, но имеют важные отличия, которые надо учитывать при выборе мер защиты.

Типовые различия:

– некоторые протоколы беспроводной безопасности несовершенны и имеют известные недостатки;

– невозможность резервного копирования информации, хранящейся на мобильных устройствах, из-за ограниченной сетевой пропускной способности или отсутствия подключения мобильных устройств во время запланированного копирования.

Удалённая работа

Меры и средства

Должна быть принята политика и меры по обеспечению ИБ для защиты доступа к информации, ее обработки и хранения при удаленной работе.

Рекомендации по реализации

Организация, использующая удаленную работу, должна разработать политику, определяющую условия и ограничения такой работы. При этом необходимо принимать во внимание следующее:

– существующую физическую безопасность места удаленной работы, включая физическую безопасность здания и окружающей среды;

– предлагаемые условия удаленной работы;

– требования в отношении безопасности коммуникаций, учитывая потребность в удаленном доступе к внутренним системам организации, чувствительность информации, к которой будет осуществляться доступ, и чувствительность внутренней системы;

– внедрение доступа к виртуальному рабочему столу, предотвращающего обработку и хранение информации на личном оборудовании;

– угрозу несанкционированного доступа к информации или ресурсам со стороны других лиц, находящихся в месте удаленной работы, например членов семьи и друзей;

– использование домашних компьютерных сетей, а также требования или ограничения в отношении конфигурации услуг беспроводных сетей;

– политики и процедуры защиты прав интеллектуальной собственности, разработанной на личном оборудовании;

– доступ к личному оборудованию, который может быть запрещен законодательно (для определения безопасности машины или на время расследования);

– лицензионные соглашения в отношении ПО, что касается ответственности за лицензирование клиентского ПО на рабочих станциях, являющихся личной собственностью сотрудников или внешних организаций;

– требования в отношении антивирусной защиты и межсетевых экранов.

Руководства и соглашения должны содержать следующее:

– предоставление необходимого оборудования и материалов для удаленной работы, где используется личное оборудование, не контролируемое организацией;

– определение разрешенной работы, часов работы, внутренних систем и сервисов, задействованных при удаленной работе, и классификация обрабатывающейся информации;

– предоставление приемлемого коммуникационного оборудования, в том числе безопасного удаленного доступа;

– физическую безопасность;

– роли и директивы семейного и гостевого доступа к оборудованию и информации;

– обслуживание и поддержку аппаратного и программного обеспечения;

– предоставление страховки;

– процедуры резервного копирования и непрерывности бизнеса;

– аудит и мониторинг безопасности;

– аннулирование пользователя, его прав доступа и возврат оборудования после завершения удаленной работы.

3. Безопасность, связанная с персоналом

Безопасность, связанную с персоналом, обеспечивают мероприятия:

– перед приемом на работу;

– во время работы;

– при увольнении или изменении должности.

3.1. Перед приемом на работу

Цель: Гарантировать, что сотрудники и подрядчики понимают свою ответственность и подходят для должностей, на которые они рассматриваются.

Перед приемом на работу проводятся следующие мероприятия:

– проверка благонадежности;

– трудовой договор.

Проверка благонадежности

Меры и средства

Тщательная проверка всех кандидатов на работу должна проводиться согласно соответствующим законам, инструкциям и правилам этики в соответствии с требованиями бизнеса, классификацией информации, к которой будет осуществляться доступ, и предполагаемыми рисками.

Рекомендации по реализации

Проверка благонадежности должна осуществляться с учетом конфиденциальности, защиты персональных данных и трудового законодательства и включать, по возможности, следующее:

– независимую проверку подлинности документов, удостоверяющих личность (паспорта или заменяющего его документа);

– проверку подлинности документов об образовании и профессиональной квалификации;

– проверку биографии кандидата (на предмет полноты и точности);

– наличие положительных рекомендаций, в частности, в отношении деловых и личных качеств претендента;

– более детальную проверку, например, кредитоспособности или наличия судимости.

Если кандидат претендует на специальную роль в сфере ИБ, организация должна удостовериться в том, что он имеет необходимую:

– компетенцию для выполнения роли;

– степень доверия, если роль критична для организации.

Если предполагаемая работа предоставляет доступ к средствам обработки информации, особенно, конфиденциальной, например, финансовой, организация должна провести дальнейшую, более детальную проверку кандидата.

Организация для процедур проверки должна определить критерии и ограничения, например, кто имеет право проверки, кто, когда и почему проводит проверку.

Процесс отбора должен также применяться и для подрядчиков. Соглашение между организацией и подрядчиком должно содержать ответственность за проведение отбора и процедуры уведомления о том, что отбор не закончен или его результаты дали повод для сомнений или опасений.

Информация обо всех кандидатах на должности в организации должна быть собрана и обработана в соответствии с действующим законодательством в этой юрисдикции. В зависимости от применяемого законодательства кандидаты должны быть заблаговременно уведомлены о действиях по отбору.

Трудовой договор

Меры и средства

Трудовой договор должен устанавливать ответственность сотрудника и подрядчика и организации в сфере ИБ.

Рекомендации по реализации

Условия работы сотрудников и подрядчиков должны отражать политику ИБ и, кроме того, разъяснять и устанавливать:

– необходимость подписания соглашения о конфиденциальности или неразглашении прежде, чем им будет предоставлен доступ к конфиденциальной информации;

– правовую ответственность и права, например в части законодательства о защите персональных данных или авторском праве;

– обязанности по классификации информации и управлению активами, связанными с информацией, средствами обработки информации и информационными сервисами;

– ответственность за обработку информации, получаемой от других фирм и сторонних организаций;

– действия, которые должны быть предприняты в случае несоблюдения требований ИБ.

Роли и ответственности в сфере ИБ должны быть доведены до кандидатов до их приема на работу.

Организация должна удостовериться, что сотрудники и подрядчики согласны с условиями ИБ в отношении вида и уровня получаемого доступа к активам, связанным с ИС и сервисами.

При необходимости ответственность, возлагаемая на сотрудника по условиям работы, должна сохраняться сотрудником в течение определенного периода времени и после увольнения из организации.

Организация в соответсвии со своим имиджем и репутацией может разработать кодекс поведения сотрудника и подрядчика, устанавливающий его обязанности в сфере ИБ в отношении конфиденциальности, защиты персональных данных, этики, допустимого использования оборудования и устройств организации.

3.2. Во время работы

Цель: Гарантировать, что все сотрудники и подрядчики осведомлены о своей ответственности и корректно выполняют свои обязанности в сфере ИБ.

Во время работы ИБ обеспечивают следующие составляющие:

– ответственность руководства;

– осведомленность в сфере ИБ;

– дисциплинарный процесс.

Ответственность руководства

Меры и средства

Руководство должно требовать от всех сотрудников и подрядчиков соблюдения правил ИБ в соответствии с установленными политиками и процедурами организации.

Рекомендации по реализации

Руководство обязано обеспечить уверенность в том, что сотрудники и подрядчики:

– осведомлены о своих ролях и обязанностях в сфере ИБ прежде, чем получили доступ к конфиденциальной информации или ИС;

– обеспечены рекомендациями по формулированию их предполагаемых ролей в сфере ИБ в рамках организации;

– заинтересованы следовать политике ИБ организации;

– достигли уровня осведомленности в сфере ИБ, соответствующего их ролям и обязанностям в организации;

– следуют условиям работы, которые включают политику ИБ организации и соответствующие методы работы;

– продолжают поддерживать соответствующие навыки и квалификацию и обучаются на регулярной основе;

– осведомлены о необходимости информирования любым способом о нарушениях политик и процедур ИБ.

Руководство должно демонстрировать поддержку политик, процедур и мер ИБ и быть образцом для подражания.

Осведомленность персонала

Меры и средства

Все сотрудники организации и, по возможности, подрядчики должны проходить соответствующее обучение и быть в курсе актуальных организационных политик и процедур, применимых к их функциям.

Рекомендации по реализации

Программа обучения должна преследовать цель осведомленности сотрудников и, по возможности, подрядчиков о своих обязанностях в сфере ИБ и мерах по их выполнению.

Программа обучения разрабатывается в соответствии с политиками и процедурами ИБ для изучения информации, которую надо защищать, и мер, которые ее должны защищать. Программа должна содержать ряд таких учебно-воспитательных мер, как акция (например, «День ИБ») и издание информационных буклетов и бюллетеней.

Программа должна планироваться, исходя из ролей сотрудников организации и, по возможности, желаемой в организации осведомленности подрядчиков. Все меры программы должны быть распланированы по времени, желательно регулярно, таким образом, чтобы они повторялись и охватывали новых сотрудников и подрядчиков. Программа должна также регулярно обновляться в соответствии с организационными политиками ипроцедурами и строиться с учетом извлечения уроков из инцидентов ИБ.

Обучение должно проходить в соответствии с программой. При обучении можно использовать разные способы и средства, включая аудиторные и дистанционные, веб-сайты, самостоятельные и другие.

Обучение в сфере ИБ должно также охватывать такие аспекты, как:

– утверждение приверженности руководства ИБ во всей организации;

– необходимость ознакомления с применяемыми правилами и обязательствами ИБ и их выполнения в соответствиис политиками, стандартами, законами, нормативами, контрактами и соглашениями;

– персональная ответственность за каждое свое действие и его отсутствие и общие ответственности за безопасность и защиту информации, принадлежащей организации и сторонним организациям;

– базовые процедуры ИБ (такие как оповещение об инциденте ИБ) и основные меры защиты (такие как аутентификация, антивирус, чистый рабочий стол);

– контактные источники дополнительной информации и консультация по мерам ИБ, включая дополнительные материалы по обучению в сфере ИБ.

Обучение должно происходить периодически. Те, кто получил новую должность или роль, к которой предъявляются другие требования ИБ, должны пройти обучение сначала с учетом новых требований (но не как новички) до начала выполнения своих ролей.

Организация должна разработать программу обучения таким образом, чтобы обучение было эффективным. Программа должна содержать разные формы обучения, например, лекционные и самостоятельные.

При составлении программы важно учитывать не только «что» и «как», но и «почему». Важно, чтобы сотрудники понимали цель ИБ и потенциальное позитивное и негативное влияние на организацию из-за их поведения.

Обучение в сфере ИБ может быть частью других процессов обучения или проведена во взаимодействии с ними, например в сфере ИТ или общей безопасности. Обучение должно соответствовать индивидуальным ролям, ответственностям и навыкам.

Оценка понимания сотрудников должна проводиться по завершении курса обучения для проверки уровня знаний.

Дисциплинарный процесс

Меры и средства

Должен существовать формальный и известный дисциплинарный процесс для принятия мер в отношении сотрудников, допустивших нарушение ИБ.

Рекомендации по реализации

Не следует начинать дисциплинарный процесс, не получив предварительного подтверждения того, что нарушение ИБ произошло.

Дисциплинарный процесс призван обеспечить уверенность в корректном и справедливом рассмотрении дел сотрудников, подозреваемых в совершении нарушений ИБ. Он должен обеспечивать дифференцированное реагирование, учитывающее такие факторы, как тип и тяжесть нарушения и его негативное влияние на бизнес, совершено ли нарушение впервые или повторно, получил ли нарушитель должную подготовку, законодательство, бизнес-контракты и другие требуемые факторы.

Дисциплинарный процесс должен использоваться как сдерживающий фактор для предотвращения нарушений сотрудниками политик и процедур ИБ и любых других нарушений ИБ организации. Преднамеренные нарушения требуют немедленных действий.

Дисциплинарный процесс может также стать мотивом или стимулом для уважительного отношения к требованиям ИБ.

3.3. Увольнение или изменение должности

Цель: Защищать интересы организации при увольнении или изменении должности сотрудника.

Увольнение или изменение обязанностей

Меры и средства

Ответственности и обязанности в сфере ИБ, которые остаются в силе после увольнения или изменения должности, должны быть определены, доведены до сотрудника или подрядчика и реализованы.

Рекомендация по реализации

Информирование об обязанностях при увольнении должно включать в себя актуальные требования ИБ и правовую ответственность и, при необходимости, обязанности, содержащиеся в соглашении о конфиденциальности, и условия трудоустройства, продолжающие действовать в течение определенного периода времени после увольнения сотрудника или подрядчика.

Ответственности и обязанности, которые остаются в силе после увольнения, должны быть включены в условия трудового договора сотрудника или контракта подрядчика.

Изменения обязанностей и условий труда должны приводить к расторжению существующего и заключению нового трудового договора, в котором будут установлены новые обязанности и условия труда.

4. Управление активами

Управление активами определяют следующие составляющие:

– ответственность за активы;

– безопасность активов;

– безопасность носителей информации.

4.1. Ответственность за активы

Цель: Определить активы организации и соответствующие ответственности по их защите.

Ответственность за активы обеспечивают следующие мероприятия:

– инвентаризация активов;

– принадлежность активов;

– использование активов;

– возврат активов.

Инвентаризация активов

Меры и средства

Организация должна идентифицировать активы, связанные с информацией и средствами для обработки информации, составить и вести их инвентарную опись.

Рекомендации по реализации

Организация должна идентифицировать все активы с учетом важности жизненного цикла информации и документа. Жизненный цикл информации состоит из создания, обработки, хранения, передачи, уничтожения и разрушения. Документация должна быть надлежащим образом внесена в существующие или новые описи.

Опись актива должна быть аккуратной, актуальной, последовательной и совместимой с другими описями.

Владение активом и классификация информации должны быть определены в отношении каждого актива.

Описи активов помогают обеспечивать уверенность в том, что активы организации эффективно защищены. Эти описи могут также потребоваться для других целей, таких как обеспечение безопасности труда, страховые или финансовые вопросы.

Принадлежность активов

Меры и средства

Активы, содержащиеся в описи, должны иметь владельцев.

Рекомендации по реализации

Физические лица, также как и другие субъекты, возложившие на себя одобренную руководством ответственность за жизненный цикл актива, квалифицируются как его владельцы.

Как правило, используется процесс временного назначения владения активом. Владение должно быть назначено, когда активы созданы и переданы организации. Владелец актива должен нести ответственность за надлежащее управление активом на протяжении всего его жизненного цикла.

Владелец актива должен:

– удостовериться, что активы инветаризированы;

– удостовериться, что активы надлежащим образом классифицированы и защищены;

– определять и пересматривать ограничения и классификации актива для важных активов с учетом применяемых правил разграничения доступа;

– принять надлежащие меры в случае уничтожения или разрушения актива.

В сложных ИС можно выделить группы активов, участвующих в обеспечении определенного сервиса. В этом случае владелец сервиса несет ответственность за обеспечение сервиса, включая работу этих активов.

Использование активов

Меры и средства

Правила использования информации и активов, связанных с информацией и средствами ее обработки, должны быть определены, задокументированы и внедрены.

Рекомендации по реализации

Сотрудники и представители внешних организаций, использующие или имеющие доступ к активам организации, должны быть осведомлены о требованиях ИБ в отношении активов организации, связанных с информацией, ресурсами и средствами ее обработки. Они должны нести ответственность за использование ими любых ресурсов для обработки информации и любое подобное использование в сфере их ответственности.

Возврат активов

Меры и средства

Все сотрудники организации и представители внешних организаций обязаны возвратить все активы организации, которые им были выданы, после окончания трудового договора, контракта или соглашения.

Рекомендации по реализации

Процесс увольнения должен быть формализован таким образом, чтобы включать в себя возврат ранее выданных физических и электронных активов, числящихся за организацией.

Если сотрудник или представитель внешней организации купил оборудование организации или пользуется личным оборудованием, при увольнении необходимо предусмотреть процедуры по возврату информации организации и надежному ее удалению на этом оборудовании.

Если сотрудник или представитель внешней организации знает важную информацию по обеспечению непрерывности операций, она быть задокументирована и передана организации.

Во время увольнения организация должна контролировать несанкционированное копирование соответствующей информации (например, интеллектуальной собственности) увольняемыми.

4.2. Безопасность информации

Цель: Обеспечить надлежащий уровень защиты информации в соответствии с ее важностью для организации.

Безопасность активов обеспечивают следующие мероприятия:

– классификация информации;

– маркировка информации;

– обработка активов.

Классификация информации

Меры и средства

Информация должна быть классифицирована с учетом правовых требований, ценности, критичности и чувствительности к несанкционированному разглашению или модификации.

Рекомендации по реализации

Классификации и меры защиты информации должны соответствовать требованиям бизнеса по распространению и ограничению информации с учетом правовых норм. Классификация активов может отличаться от классификации информации, которая хранится, обрабатывается и защищается активом, но при этом должна быть с нею согласована.

Владельцы информационных активов должны нести ответственность за их классификацию.

Схема классификации информации должна содержать правила и критерий пересмотра классификации с течением времени. Уровень защиты в схеме должен быть установлен путем анализа конфиденциальности, целостности и доступности и других требований к информации. Схема должна соответствовать правилам разграничения доступа.

Информация может перестать быть конфиденциальной по истечении некоторого периода времени и становится общедоступной. Эти аспекты необходимо принимать во внимание, поскольку присвоение более высокой категории может привести к реализации избыточных мер защиты и, как следствие, дополнительным расходам.

Каждый уровень должен иметь название в контексте применения схемы классификации.

Схема должна способствовать во всей организации тому, чтобы каждый мог классифицировать информацию и связанные с ней активы, иметь общее понимание требований защиты и применять надлежащую защиту.

Классификация должна быть включена в процессы организации и быть согласованной по всей организации. Результаты классификации должны показывать ценность активов в зависимости от их чувствительности и критичности для организации, например, конфиденциальности, целостности и доступности. Результаты классификации должны обновляться в соответствии с изменениями ценности, чувствительности и критичности активов на протяжении всего их жизненного цикла.

Классификацию проводят люди, работающие с информацией и четко осознающие, как ее обрабатывать и защищать. Создание информационных групп со схожей защитой требует и определяет процедуры ИБ, применимые для всей информации в каждой группе. Такой подход снижает необходимость оценки риска и поиска мер защиты в каждом конкретном случае.

Информация может перестать быть чувствительной или критичной после определенного периода времени, например, когда станет публичной. Такие аспекты надо принимать во внимание, поскольку избыточная классификация может приводить к внедрению ненужных мер защиты и дополнительным расходам, а недостаточная – подвергать опасности достижение бизнес-целей.

Схема классификации конфиденциальности информации может содержать, например, четыре следующих уровня:

– разглашение не приносит вреда;

– разглашение вызывает небольшое затруднение и оперативное неудобство;

– разглашение имеет серьезное короткое влияние на операции или тактические цели;

– разглашение имеет серьезное влияние на долговременные стратегические цели или подвергает деятельность организации риску.

Маркировка информации

Меры и средства

Соответствующий набор процедур маркировки информации должен быть разработан и внедрен в соответствии со схемой ее классификации, принятой в организации.

Рекомендации по реализации

Процедуры маркировки должны охватывать информацию и связанные с ней активы как в физической, так и в электронной форме. Маркировка должна отражать установленную схему классификацию. Метки должны быть легко распознаваемыми.

Процедуры должны указывать, где и как наносить метки с учетом видов доступа к информации или обработки активов в зависимости от типов носителя. Процедуры должны определять, когда маркировка не применяется, например, для неконфиденциальной информации, для снижения нагрузок.

Сотрудники и подрядчики должны быть осведомлены о процедурах маркировки.

Выходные данные ИС, содержащие информацию, классифицированную как чувствительную или критичную, должны иметь соответствующую классификационную метку.

Маркировка классифицированной информации является ключевым требованием для соглашений по распространению информации. Физические метки и метаданные являются общепризнаной формой маркировки.

Обработка активов

Меры и средства

Процедуры обработки активов должны быть разработаны и внедрены в соответствии со схемой классификации информации, принятой в организации.

Рекомендации по реализации

Процедуры должны быть установлены для обработки, хранения и передачи информации в соответствии с ее классификацией.

Необходимо рассмотреть следующие рекомендации:

– ограничения доступа в соответствии с требованиями защиты для каждого уровня классификации;

– ведение формальной записи авторизованных получателей активов;

– соответствие защиты любых копий информации уровню защиты исходной информации;

– хранение ИТ активов в соответствии с рекомендациями изготовителей;

– четкая маркировка всех копий носителей информации для авторизованного получателя.

Для каждого уровня классификации должны быть определены процедуры доступа и использования информационных активов, включающие безопасную обработку, хранение, передачу, присвоение и снятие грифа секретности, а также уничтожение. Сюда следует также отнести процедуры по обеспечению регистрации любого события, имеющего значение для ИБ, и хранению этих данных.

Сотрудники и представители внешних организаций, имеющие право доступа к активам организации, должны быть осведомлены о существующих ограничениях по использованию разных видов информационных активов в соответствии со схемой их классификации и маркировки, принятой в организации. Они должны нести ответственность за использование ими активов организации.

4.3. Безопасность носителей информации

Цель: Предотвратить несанкционированные действия с информацией, хранящейся на носителях информации.

Безопасность носителей информации обеспечивают следующие мероприятия:

– управление носителями;

– уничтожение носителей;

– транспортировка носителей.

Управление носителями

Меры и средства

Должны быть внедрены процедуры управления носителями информации в соответствии со схемой классификации, принятой в организации.

Рекомендации по реализации

Необходимо рассмотреть следующие рекомендации:

– в случае ненужности содержание перезаписываемого носителя, который будет вынесен за пределы организации, необходимо уничтожить без возможности восстановления;

– при необходимости, носители, выносимые за пределы организации, должны требовать авторизацию, и запись таких выносов следует хранить для аудита;

– все носители информации должны храниться в сейфе, безопасной среде в соответствии с рекомендациями изготовителей;

– если конфиденциальность и целостность данных считается важным, для их защиты на носителе должны использоваться средства криптографии;

– для снижения риска потери данных на старом носителе, пока он еще читаемый, необходимо их перезаписать на новый носитель;

– множественные копии ценных данных должны храниться на разных носителях для снижения риска случайного повреждения или потери данных;

– должна вестись регистрация носителей для уменьшения возможности потери данных;

– сменные дисковые накопители разрешается использовать только в случае, обусловленном потребностями бизнеса;

– там, где необходимо использование носителей, запись информации на такой носитель должна мониториться.

Процедуры и уровни авторизации должны быть задокументированы.

Уничтожение носителей

Меры и средства

Если носитель больше не нужен, он должен быть надежно уничтожен в соответствии с формальной процедурой.

Рекомендации по реализации

Формальные процедуры надежного уничтожения носителей должны буть установлены для снижения риска утечки конфиденциальной информации посторонним лицам. Процедуры надежного уничтожения носителей, содержащих конфиденциальную информацию, должны соответствовать чувствительности этой информации.

Необходимо рассмотреть следующие рекомендации:

– носители, содержащие конфиденциальную информацию, должны храниться и уничтожаться надежно, например, путем сжигания и измельчения или стирания данных для другого применения внутри организации;

– должны существовать процедуры по выявлению носителей, которые необходимо уничтожить;

– проще принять меры по сбору и уничтожению всех носителей информации, чем выявлять носители с чувствительной информацией;

– многие организации предлагают сбор и сервисы уничтожения носителей, среди них надо выбрать ту, которая имеет адекватные меры защиты и квалификацию;

– уничтожение чувствительной информации должно регистрироваться, а запись храниться для аудита.

При сборе носителей для уничтожения необходимо учитывать эффект «перехода количества в качество», который может превратить большой объем нечувствительной информации в чувствительную.

Поврежденные устройства, содержащие чувствительные данные, могут потребовать оценку риска того, были ли они достаточно физически разрушены до того, как были выброшены или попали в ремонт.

Транспортировка носителей

Меры и средства

Носители должны быть защищены от несанкционированного доступа, неправильного использования или повреждения во время транспортировки.

Рекомендации по реализации

Для защиты носителей, содержащих информацию, при транспортировке необходимо учитывать следующие рекомендации:

– должен использоваться надежный транспорт или курьеры;

– список разрешенных курьеров необходимо согласовывать с руководством;

– необходимо разработать процедуры проверки благонадежности курьеров;

– упаковка должна быть прочной для защиты содержимого от физического повреждения, возможного при транспортировке и соответствовать рекомендациям изготовителей, например, защищать от экологических факторов, снижающих эффективность восстановления носителя, таких как высокая температура, влажность или электромагнитные поля;

– должны храниться записи, определяющие содержимое носителей, применяемую защиту, а также времени передачи курьерам и доставки адресату.

Информация может быть уязвимой для несанкционированного доступа, неправильного использования или повреждения в физическом транспорте, например, при отправлении почтой или курьером. В этом случае носители должны иметь сопроводительные документы.

Если конфиденциальная информация на носителе незашифрована, должна быть применена дополнительная физическая защита носителя.

5. Управление доступом

Управление доступом определяют следующие составляющие:

– правила разграничения доступа;

– управление доступом пользователей;

– ответственность пользователя;

– управление доступом к системе и приложениям.

5.1. Требования разграничения доступа

Цель: Ограничить доступ к информации и средствам обработки информации.

Требования по управлению доступом определяют следующие составляющие:

– правила разграничения доступа;

– доступ к сетям и сетевым сервисам.

Правила разграничения доступа

Меры и средства

Правила разграничения доступа должны быть разработаны, задокументированы и пересматриваться на основе требований ИБ и бизнеса.

Рекомендации по реализации

Владельцы активов должны определить надлежащие правила разграничения доступа, права доступа и ограничения для определенных пользовательских ролей по отношению к их активам с детализацией и строгостью разграничений, отражающих соответствующие риски ИБ.

Разграничения доступа являются как логическими, так и физическими, и должны рассматриваться вместе. Пользователи и провайдеры услуг должны четко обозначить требования бизнеса, которые должны удовлетворить разграничения доступа.

Правила должны учесть следующее:

– требования к безопасности прикладных программ бизнеса;

– политики распространения информации и авторизации, например, общепризнанные принципы и уровни ИБ и классификацию информации;

– согласованность между правами доступом и политиками классификации информации систем и сетей;

– требования законодательства и договорные обязательства по ограничению доступа к данным или услугам;

– управление правами доступа в распределенных и сетевых средах, которые распознают все типы возможных соединений;

– разделение ролей разграничения доступа, например, запрос доступа, авторизация доступа, администрирование доступа;

– требования к формальной авторизации прав доступа;

– требования к периодическому пересмотру управления доступом;

– аннулирование прав доступа;

– архивирование записей всех серьезных событий по использованию и управлению удостоверениями пользователей и секретной информацией автентификации;

– роли привилегированного доступа.

При разработке правил разграничения доступа необходимо учесть следующее:

– установление правил на основании предпосылки «Запрещено все, что не разрешено» вместо «Разрешено все, что не запрещено»;

– изменения информационных меток, инициированные автоматически средствами обработки информации и по усмотрению пользователя;

– изменения пользовательских разрешений, инициированные автоматически ИС и администратором;

– наличие правил, требующих определенного утверждения перед введением в действие и не требующих.

Правила разграничения доступа должны поддерживаться формальными процедурами и определять ответственности.

Разграничение ролевого доступа является тем подходом, которым пользуются многие организации для связывания прав доступа с бизнес-ролями.

Два общепризнанных принципа правил разграничения доступа:

– *знание*: наличие доступа только к информации, необходимой для выполнения задач (разные задачи/роли означают разную потребность знаний и следовательно разный профиль доступа);

– *использование*: наличие доступа только к средствам обработки информации, необходимым для выполнения задачи/работы/роли (ИТ оборудование, приложения, процедуры, кабинеты).

Доступ к сетям и сетевым сервисам

Меры и средства

Пользователям должен предоставляться доступ к сетям и сетевым сервисам, когда они имеют официальные полномочия на это.

Рекомендации по реализации

Следует сформулировать политику использования сетей и сетевых услуг.

В политике необходимо рассмотреть:

– сети и сетевые услуги, к которым разрешен доступ;

– процедуры авторизации для определения того, кому и к каким сетям и сетевым услугам разрешен доступ;

– процедуры и средства управления по защите доступа к сетевым подключениям и сетевым услугам;

– средства доступа к сетям и сетевым услугам (например, VPN или беспроводной сети);

– требования пользовательской аутентификации для доступа к разным сетевым сервисам;

– мониторинг использования сетевых сервисов.

Политика использования сетевых сервисов должна быть согласована с правилами разграничения доступа организации.

Неавторизованные и незащищенные подключения к сетевым сервисам могут повлиять на всю организацию. Такой контроль очень важен для сетевых подключений к чувствительным и критичным бизнес-приложениям или к пользователям в местах повышенного риска, например, публичных или удаленных регионах, находящихся вне зоны контроля и управления ИБ организации.

5.2. Управление доступом пользователей

Цель: Обеспечить авторизованный доступ пользователей и предотвратить неавторизованный доступ к системам и сервисам.

Управление доступом пользователей обеспечивают следующие мероприятия:

– регистрация и ее отмена;

– предоставление доступа;

– пересмотр прав доступа;

– удаление или изменение прав доступа.

Управление доступом пользователей обеспечивает также управление следующим:

– правами привилегированного доступа;

– паролями.

Регистрация и ее отмена

Меры и средства

Формальный процесс регистрации пользователя ее отмены должен быть внедрен для предоставления прав доступа.

Рекомендации по реализации

Процесс управления идентификаторами пользователя должен включать:

– использование уникальных идентификаторов пользователя, позволяющих отследить их действия и ответственность за них; использование распространенных идентификаторов должно быть разрешено только в случае оперативной или бизнес-необходимости, задокументировано и утверждено;

– немедленную деактивацию или удаление идентификаторов пользователя после его увольнения;

– периодическую идентификацию и деактивацию или удаление ненужных идентификаторов пользователя;

– гарантию того, что деактивированные идентификаторы не достались другим пользователям.

Разрешение или запрет доступа к информации и средствам ее обработки состоит из следующих двух этапов:

– создание и активация или деактивация идентификатора пользователя;

– активация или деактивация прав доступа идентификатора пользователя.

Предоставление доступа

Меры и средства

Формальный процесс предоставления доступа должен быть внедрен для назначения или отмены прав доступа для всех типов пользователя во всех системах и сервисах.

Рекомендации по реализации

Процесс предоставления доступа должен включать:

– получение полномочий от собственника ИС или сервиса для их использования;

– проверку того, что уровень предоставленного доступа соответствует правилам доступа и другим требованиям, например, разделения обязанностей;

– гарантию того, что права доступа не будут активированы (например, провайдером услуг) до завершения процедур авторизации;

– ведение централизованной записи прав доступа, предоставленных идентификатору пользователя для доступа к ИС и сервисам;

Конец ознакомительного фрагмента.