**Тема 4: "СТАНДАРТЫ УПРАВЛЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ"**

***4.1 Стандарты управления информационной безопасностью BS 7799 и ISO/IEC Их основные положения***

Информационная безопасность представляет собой проблему высокой сложности. Обеспечение информационной безопасности нуждается в комплексном подходе к разработке средств защиты, как на техническом, так и на организационном уровне.

ИБ не может быть обеспечена разовым мероприятием, например, покупкой конкретного набора средств защиты. Арсенал средств защиты нуждается в постоянном обновлении, поскольку новые угрозы и новые уязвимости все время появляются в процессе жизненного цикла ИС. Данное обстоятельство вынуждает рассматривать обеспечение ИБ как постоянный процесс, который принято называть ***процессом управления информационной безопасностью***.

Несколько лет назад Британский Институт Стандартов (BSI) при поддержке группы коммерческих организаций приступил к разработке стандарта управления информационной безопасностью, который потом получил название BS 7799.

При разработке стандарта ставилась задача *обеспечения государственных и коммерческих организаций инструментом для создания эффективных систем информационной безопасности на основе современных методов управления*. В 2000 году этот стандарт был признан международным под названием "Международный стандарт ISO/IEC 17799 «Информационные технологии – Управление информационной безопасностью».

Стандарт ISO/IEC 17799 – это модель системы управления, которая определяет общую организацию, классификацию данных, системы доступа, направления планирования, ответственность сотрудников, использование оценки риска и т.п. в контексте информационной безопасности. В процессе внедрения стандарта создается так называемая система управления (управления) информационной безопасности, цель которой – сокращение материальных потерь, связанных с нарушением информационной безопасности. *Основная идея стандарта* – помочь коммерческим и государственным хозяйственным организациям решить достаточно сложную задачу: не только обеспечить надежную защиту информации, но также организовать эффективный доступ к данным и нормальную работу с ними.

*Структура стандарта* позволяет выбрать те средства управления, которые имеют отношение к конкретной организации или сфере ответственности внутри организации. Содержание стандарта включает следующие разделы (рис. 1):

- политика безопасности; организация защиты;

- классификация ресурсов и контроль;

- безопасность персонала;

- физическая безопасность и безопасность окружающей среды;

- администрирование компьютерных систем и вычислительных сетей;

- управление доступом к системе;

- разработка и сопровождение информационных систем;

- планирование непрерывной работы организации;

- выполнение требований (соответствие законодательству).

В связи с этим выделяется ряд ключевых элементов управления, которые представляются как фундаментальные:

- политика информационной безопасности;

- распределение ответственности за информационную безопасность;

- образование и тренинг по информационной безопасности;

- отчетность за инциденты по безопасности;

- защита от вирусов;

- обеспечение непрерывности работы;

- контроль копирования лицензионного программного обеспечения;

- защита архивной документации организации;

- защита персональных данных;

- реализация политики информационной безопасности.

Как видно, наряду с элементами управления для компьютеров и компьютерных сетей, стандарт уделяет большое внимание вопросам разработки политики безопасности, работе с персоналом (прием на работу, учебу, освобождение от работы), обеспечению непрерывности производственного процесса, юридическим требованиям.

Безусловно, что не все 109 пунктов стандарта можно применять в условиях абсолютно каждой организации. Поэтому авторами стандарта был выбран подход, при котором стандарт используется как некоторое "меню", из которого следует выбрать элементы, которые можно применить для конкретных условий. Этот выбор осуществляется на основе оценки риска и тщательным образом обосновывается.

**Риск определяется как произведение показателя возможных потерь (ущерба) на вероятность того, что эта потеря произойдет**. Под потерями понимают материальные потери, связанные с нарушением следующих свойств информационного ресурса:

- конфиденциальность – защищенность информации от несанкционированного доступа;

- целостность – защищенность информации от несанкционированного изменения, обеспечения ее точности и полноты;

- доступности возможность использования информации, когда в этом возникает необходимость, работоспособность системы.

Стандарт не сосредотачивается только на обеспечении конфиденциальности.

* В коммерческих организациях, с точки зрения материальных потерь, вопросы целостности и доступности чаще всего более весомые. В упрощенном виде анализ риска сводится к ответам на следующие вопросы:
* Что может угрожать информационным ресурсам?
* Какова уязвимость этим угрозам, то есть, что может произойти с тем или другим информационным ресурсом?
* Если это произойдет, то насколько тяжелыми будут последствия?
* Какие возможны убытки? Как часто следует ожидать подобные случаи?

В настоящее время, разработана следующая версия данного стандарта

***4.2. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования"***

Информационная безопасность тесно связана с работой бизнеса, его конкурентоспособностью, успешностью имиджа предприятия и, в конечном итоге, доходами компании. Лучшей мировой практикой в области управления информационной безопасностью признан стандарт ISO/IEC 27001:2005.

*Область применения*

Все виды организаций (например, коммерческие и некоммерческие организации, правительственные организации)

*Определяет требования к средствам контроля безопасности, специально разработанные для нужд организации, или ее части.*

Цель – выбор адекватных и соразмерных средств контроля ИБ, которые защищают информационные активы и предоставляют уверенность заинтересованным сторонам.

Назначение:

**Устанавливает требования к системе управления информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы**.

Основа стандарта ИСО 27001 – система управление рисками, связанными с информацией.

Система управления рисками позволяет получать ответы на следующие вопросы:

- На каком направлении информационной безопасности требуется сосредоточить внимание?

- Сколько времени и средств можно потратить на данное техническое решение для защиты информации?

Менеджмент рисков происходит по классической схеме: поиск, классификация, ранжирование, оценка, план по снижению рисков, принятие остаточных рисков и регулярный пересмотр рисков.

*Общие положения стандарта:*

Данный Стандарт определяет информационную безопасность как: "сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность".

Основной задачей информационной безопасности является защита информационных ресурсов компании от внутренних и внешних умышленных и неумышленных угроз (подделка, вандализм, кража, пожар, системный сбой и др.).

Целью информационной безопасности является обеспечение непрерывности бизнеса компании и минимизация бизнес-рисков путем предупреждения инцидентов безопасности и уменьшения размеров потенциального ущерба.

Стандарт определяет следующие аспекты информационной безопасности:

- Конфиденциальность – обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи);

- Целостность – обеспечение точности и полноты информации, а также методов ее обработки;

- Доступность – обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию).

Структура стандарта

Общие положения:

1. Область применения

2. Нормативные ссылки

3. Термины и определения

4. Система информационной безопасности

5. Обязательства руководства

6. Внутренние аудиты системы управления

7. Анализ системы управления информационной безопасности руководством

8. Совершенствование системы управления информационной безопасности

*Процессный подход*

Стандарт декларирует два основных принципа управления:

1 Процессный подход к управлению безопасностью, который рассматривает управление как процесс – набор взаимосвязанных непрерывных действий, акцентирует внимание на достижении поставленных целей, а также ресурсах, затраченных для достижения целей.

2. Применение PDCA модели как основы для всех процедур управления ИБ. PDCA модель (или модель Шухарта-Деминга) определяет четыре этапа, которые должны выполняться последовательно для каждого процесса.



***Рис. 4 Применение PDCA***

Создание и эксплуатация СУИБ требует применения такого же подхода, как и любая другая система управления. Используемая в ISO для описания СУИБ процессная модель предусматривает непрерывный цикл мероприятий: планирование, реализация, проверка, действие (ПРПД).

Процессная модель включает 4 группы процессов:

1) Планирование.2) Реализация. 3) Проверка. 4) Действие.

На стадии планирования обеспечивается правильное задание контекста и масштаба СУИБ, оцениваются риски информационной безопасности, предлагается соответствующий план обработки этих рисков. В свою очередь, на стадии реализации внедряются принятые решения, которые были определены на стадии планирования. На стадиях проверки и действия усиливают, исправляют и совершенствуют решения по безопасности, которые уже были определены и реализованы.

*Этапы создания СУИБ*

*В соответствии с процессной моделью, стандарт определяет 4 этапа создания СУИБ*.

1. На этапе "***Разработка системы управления информационной безопасности***" организация должна осуществить следующее:

1) определить область и границы действия СУИБ;

2) определить политику СУИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий;

3) определить подход к оценке риска в организации;

4) идентифицировать риски;

5) проанализировать и оценить риски;

6) определить и оценить различные варианты обработки рисков;

7) выбрать цели и меры управления для обработки рисков;

8) получить утверждение руководством предполагаемых остаточных рисков;

9) получить разрешение руководства на внедрение и эксплуатацию СУИБ;

10) подготовить Положение о применимости.

2. Этап "***Внедрение и функционирование системы управления информационной безопасности***" предполагает, что организация должна выполнить следующее:

1) разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении управления рисков ИБ;

2) реализовать план обработки рисков для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределение функций и обязанностей;

3) внедрить выбранные меры управления;

4) определить способ измерения результативности выбранных мер управления;

5) реализовать программы по обучению и повышению квалификации сотрудников;

6) управлять работой СУИБ;

7) управлять ресурсами СУИБ;

8) внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ.

3. Третий этап "***Проведение мониторинга и анализа системы управления информационной безопасности***" требует:

1) выполнять процедуры мониторинга и анализа;

2) проводить регулярный анализ результативности СУИБ;

3) измерять результативность мер управления для проверки соответствия требованиям ИБ;

4) пересматривать оценки рисков через установленные периоды времени, анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения;

5) проводить внутренние аудиты СУИБ через установленные периоды времени;

6) регулярно проводить руководством организации анализ СУИБ в целях подтверждения адекватности ее функционирования и определения направлений совершенствования;

7) обновлять планы ИБ с учетом результатов анализа и мониторинга;

8) регистрировать действия и события, способные повлиять на результативность или функционирование СУИБ.

4. И наконец, этап "***Поддержка и улучшение системы управления информационной безопасности***" предполагает, что организация должна регулярно проводить следующие мероприятия:

1) выявлять возможности улучшения СУИБ;

2) предпринимать необходимые корректирующие и предупреждающие действия, использовать на практике опыт по обеспечению ИБ, полученный как в собственной организации, так и в других организациях;

3) передавать подробную информацию о действиях по улучшению СУИБ всем заинтересованным сторонам, при этом степень ее детализации должна соответствовать обстоятельствам и, при необходимости, согласовывать дальнейшие действия;

4) обеспечивать внедрение улучшений СУИБ для достижения запланированных целей.

Далее в стандарте приводятся требования к документации, которая в частности должна включать положения политики СУИБ и описание области функционирования, описание методики и отчет об оценке рисков, план обработки рисков, документирование связанных процедур. Также должен быть определен процесс управления документами СУИБ, включающий актуализацию, использование, хранение и уничтожение.

Для предоставления свидетельств соответствия требованиям и результативности функционирования СУИБ необходимо вести и поддерживать в рабочем состоянии учетные записи и записи о выполнении процессов. В качестве примеров называются журналы регистрации посетителей, отчеты о результатах аудита и т.п.

Стандарт определяет, что руководство организации ответственно за обеспечение и управление ресурсами, необходимыми для создания СУИБ, а также организацию подготовки персонала.

Как уже ранее отмечалось, организация должна в соответствии с утвержденным графиком проводить внутренние аудиты СУИБ, позволяющие оценить ее функциональность и соответствие стандарту. А руководство должно проводить анализ системы управления информационной безопасности.

Также должны проводиться работы по улучшению системы управления информационной безопасности: повышению ее результативности и уровня соответствия текущего состояния системы и предъявляемым к ней требованиям.

В приложении к стандарту перечисляются рекомендуемые меры управления, взятые из ранее рассмотренного стандарта ISO/IEC 17799:2005.

Наряду с элементами управления для компьютеров и компьютерных сетей, стандарт уделяет большое внимание вопросам разработки политики безопасности, работе с персоналом (прием на работу, обучение, увольнение с работы), обеспечению непрерывности производственного процесса, юридическим требованиям.

***4.3 Сертификация СУИБ на соответствие ISO 27001***

Для подтверждения соответствия существующей в организации СУИБ требованиям стандарта, а также ее адекватности существующим бизнес рискам используется процедура добровольной сертификации.

ISO 27001:2005 является стандартом, по которому проводится официальная сертификация СУИБ. Стандарт представляет собой перечень требований, обязательных для сертификации.

Под сертификацией системы управления информационной безопасностью (СУИБ) организации по требованиям стандарта ISO 27001:2005 понимается комплекс организационно-технических мероприятий, проводимых независимыми экспертами, в результате чего подтверждается наличие и надлежащее функционирование всех рекомендуемых стандартом механизмов контроля, применимых в данной организации.

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), что укрепляет имидж компании, повышает интерес со стороны потенциальных клиентов, инвесторов, кредиторов и спонсоров.

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 информационной безопасности областях, такой, например, как финансы, наличие сертификата соответствия ISO начинает выступать как обязательное требование для осуществления деятельности. Некоторые российские компании уже сталкиваются с этими ограничениями.

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 системе управления информационной безопасностью, что в перспективе означает для организации снижение среднестатистического ущерба от инцидентов безопасности, а также сокращение накладных расходов на эксплуатацию информационных систем. Вполне возможно, наличие сертификата позволит застраховать информационные риски организации на более выгодных условиях.

Как свидетельствует текущая практика, расходы на сертификацию в большинстве случаев несопоставимо малы в сравнении с затратами организации на обеспечение информационной безопасности, а получаемые преимущества многократно их компенсируют.

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.

Для получения сертификата система управления информационной безопасности предприятия оценивается аудитором. Аудит состоит из анализа документации по системе управления информационной безопасности, а также выборочного контроля в организации, который позволяет удостовериться, что реальная практика отвечает описанию системы.

Аккредитованную сертификацию могут осуществлять лишь те сертификационные общества, которые прошли аккредитацию ISO. Сертификат, выданный такой организацией, признается на международном уровне.

Сертификация на соответствие стандарту ISO 27001:2005 позволяет наглядно показать деловым партнерам, инвесторам и клиентам, что в компании налажено эффективное управление информационной безопасностью. В свою очередь это обеспечивает компании конкурентное преимущество, демонстрируя способность управлять информационными рисками, при этом также увеличивается капитализация компании.

***Выгоды внедрения системы управления информационной безопасности по требованиям стандарта ISO/IEC 27001:2005***

Система управления информационной безопасностью на основе стандарта ISO позволит:

Сделать большинство информационных активов наиболее понятными для управления компании.

Выявлять основные угрозы безопасности для существующих бизнес-процессов.

Рассчитывать риски и принимать решения на основе бизнес-целей компании.

Обеспечить эффективное управление системой в критичных ситуациях.

Проводить процесс выполнения политики безопасности (находить и исправлять слабые места в системе информационной безопасности).

Четко определить личную ответственность.

Достигнуть снижения и оптимизации стоимости поддержки системы безопасности.

Продемонстрировать клиентам, партнерам, владельцам бизнеса свою приверженность к информационной безопасности.

Получить международное признание и повышение авторитета компании, как на внутреннем рынке, так и на внешних рынках.

Подчеркнуть прозрачность и чистоту бизнеса перед законом благодаря соответствию стандарту.