**Тема 5: "СОЗДАНИЕ СУИБ НА ПРЕДПРИЯТИИ"**

***5.1. Этапы создания системы управления ИБ***

Для начала отметим, что создание СУИБ на предприятии и подготовка к ее сертификации на соответствие требованиям стандарта ISO27001, как правило, делится на два основных этапа:

- разработку системы управления (и всех необходимых процедур);

- внедрение системы управления.

Для выполнения первого этапа рекомендуется приглашать консультантов. Второй этап (внедрение) выполняется самой компанией (специалисты компании должны ознакомиться с необходимыми процедурами, наладить их четкое выполнение, проверять и контролировать их эффективность и пр.).

Можно выделить следующие **основные этапы разработки** системы управления ИБ:

1) инвентаризация активов;

2) категорирование активов;

3) оценка защищенности информационной системы;

4) оценка информационных рисков;

5) обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов);

6) внедрение выбранных мер обработки рисков;

7) контроль выполнения и эффективности выбранных мер.

**Роль руководства компании в системе управления ИБ**

Одним из основных условий эффективного функционирования системы управления ИБ является вовлеченность руководства компании в процесс управления ИБ. Все сотрудники должны понимать, что, во-первых, вся деятельность по обеспечению ИБ инициирована руководством и обязательна для выполнения, во-вторых, руководство компании лично контролирует функционирование системы управления ИБ, в-третьих, само руководство выполняет те же правила по обеспечению ИБ, что и все сотрудники компании.

**Выбор области сертификации**

Систему управления ИБ, как правило, целесообразно разрабатывать для всей компании в целом. Другими словами, процедуры системы управления в большинстве случаев необходимы для выполнения во всей компании. Однако внедрить систему управления сразу во все бизнес-процессы часто непросто, поэтому лучше, если ее внедрение будет осуществляться последовательно. Таким образом, внедрив систему управления в каком-то одном бизнес-процессе компании, мы можем получить сертификат на нее в рамках данного бизнес-процесса, а затем расширять область сертификации по мере внедрения в остальные процессы компании. Следовательно, при подготовке к сертификации требуется определить область сертификации (описать, в какой конкретно подсистеме компании будет внедрена система управления). Аудиторы сертификационных органов проверяют выполнение всех процедур системы управления только в рамках выбранной области сертификации.

Важно иметь в виду, что описание области сертификации необходимо выполнить максимально подробно, то есть требуется точно определить активы, входящие в область сертификации.

***Содержание этапов разработки и внедрения системы управления ИБ***.

**1.Инвентаризация активов компании**

Прежде всего, следует определить, что является ценным активом компании с точки зрения информационной безопасности. Стандарт ISO 17799, подробно описывающий процедуры системы управления ИБ, выделяет следующие виды активов:

- информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.);

- программное обеспечение,

- материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.);

- сервисы (поддерживающая инфраструктура);

сотрудники компании, их квалификация и опыт,

нематериальные ресурсы (репутация и имидж компании).

Следует определить, нарушение информационной безопасности, каких активов может нанести ущерб компании. В этом случае актив будет считаться ценным, и его необходимо будет учитывать при анализе информационных рисков.

Инвентаризация заключается в составлении перечня ценных активов компании. Как правило, данный процесс выполняют владельцы активов.

***5.2 Категорирование активов компании***

В процессе категорирования активов необходимо оценить их критичность для бизнес-процессов компании или, другими словами, определить, какой ущерб понесет компания в случае нарушения информационной безопасности активов.

Данный процесс вызывает наибольшую сложность, так как ценность активов определяется на основе экспертных оценок их владельцев. В процессе данного этапа часто проводятся обсуждения между консультантами по разработке системы управления и владельцами активов. Это помогает последним понять, каким образом следует определять ценность активов с точки зрения информационной безопасности (как правило, процесс определения критичности активов является для владельца новым и нетривиальным). Кроме этого, для владельцев активов разрабатываются различные методики оценки. В частности, такие методики могут содержать конкретные критерии (актуальные для данной компании), которые следует учитывать при оценке критичности.

Оценка критичности активов выполняется по трем параметрам: конфиденциальности, целостности и доступности (следует оценить ущерб, который понесет компания при нарушении конфиденциальности, целостности или доступности активов).

Оценку критичности активов можно выполнять в денежных единицах и в уровнях. Однако, учитывая тот факт, что для анализа информационных рисков необходимы значения в денежных единицах, в случае оценки критичности активов в уровнях, следует определить оценку каждого уровня в деньгах. Например, для базовой оценки рисков достаточно 3-уровневой шкалы оценки критичности - низкий, средний и высокий уровни.

При выборе шкалы важно учитывать следующее:

чем меньше количество уровней, тем ниже точность оценки;

чем больше количество уровней, тем выше сложность оценки (то есть сложно определить разницу между, скажем, 7-м и 8-м уровнем 10-ти уровневой шкалы).

Следовательно, в этом вопросе нужно найти «золотую середину», чтобы и точность не очень пострадала, и сложность не превышала допустимых пределов.

Кроме этого, следует иметь в виду, что для расчета информационных рисков достаточно примерных значений критичности активов: не обязательно оценивать их с точностью до денежной единицы. Однако денежное выражение критичности все равно необходимо.

Рассмотрим подробнее принципы оценки критичности каждого указанного актива.

- Информационные активы (или виды информации) оцениваются с точки зрения нанесения компании ущерба от их раскрытия, модификации или недоступности в течение определенного времени.

- Программное обеспечение, материальные ресурсы и сервисы оцениваются, как правило, с точки зрения их доступности или работоспособности. То есть требуется определить, какой ущерб понесет компания при нарушении функционирования данных активов. Например, нарушение системы кондиционирования в течение трех суток приведет к отказу серверов компании, к ним будет нарушен доступ, и вследствие этого компания понесет убытки.

- Сотрудники компании с точки зрения конфиденциальности и целостности оцениваются, учитывая их доступ к информационным ресурсам с правами на чтение и на модификацию. Доступность сотрудников оценивается с точки зрения их отсутствия на рабочем месте. Другими словами, оценивается, какой ущерб понесет компания при отсутствии сотрудника в течение определенного периода времени. Здесь важно учесть опыт сотрудника, его квалификацию, выполнение им каких-либо специфических операций.

- Репутация компании оценивается в связи с информационными ресурсами: какой ущерб репутации компании будет нанесен в случае нарушения безопасности информации компании.

Заметим, что процесс категорирования активов должен подчиняться четким документированным процедурам компании. Аудиторам сертификационного органа будет недостаточно формального документа, отражающего результаты категорирования. От владельцев активов требуется, чтобы они могли объяснить, какие методики они использовали при оценке, на основании каких данных были получены результаты оценки.

***5.3 Оценка защищенности информационной системы компании***

Очевидно, что для анализа информационных рисков необходимо оценить не только критичность активов, но и уровень их защищенности.

В процессе оценки защищенности информационной системы определяются угрозы, действующие на активы, а также уязвимости информационной системы, в которой обрабатываются активы и которые могут привести к реализации угроз. Угрозы и уязвимости рассматриваются только во взаимосвязи друг с другом. Уязвимость, через которую невозможно реализовать ни одну из угроз, не имеет смысла. Аналогично, угроза, которую невозможно реализовать ввиду отсутствия уязвимости, также неактуальна.

Не вызывает сомнения, что различные угрозы и уязвимости имеют разное значение (разный вес) для информационной системы. Например, злоумышленник скорее решит воспользоваться открытой дверью, чем открытым окном, если офис компании расположен на семнадцатом этаже 34-этажного здания (однако совсем исключать вторую возможность не стоит). Следовательно, необходимо определить, какие угрозы и уязвимости наиболее актуальны, а какие менее значимы, или, другими словами, определить вероятность реализации угрозы через уязвимость. Вероятность реализации уязвимостей (как и любая другая вероятность) определяется в пределах от 0 до 1 (или от 0 до 100 %).

Угрозы, уязвимости, а также их вероятности определяются в результате проведения технологического аудита защищенности информационной системы компании. Такой аудит может быть выполнен как специалистами компании (так называемый, внутренний аудит), так и сторонними консультантами (внешний аудит).

***5.4 Оценка информационных рисков***

Оценка информационных рисков заключается в расчете рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей.

Классическая формула оценки рисков:

**R=D Р( V)**

где R – информационный риск;

D – критичность актива (ущерб);

Р(V) – вероятность реализации уязвимости.

Результаты оценки рисков, как правило, представляются в «Отчете об оценке информационных рисков компании».

**Обработка информационных рисков**

Обработка информационных рисков – это этап, в процессе которого определяется, какие действия по отношению к рискам требуется выполнить в компании.

Основными способами обработки рисков являются:

- принятие рисков;

- уклонение от рисков;

- передача рисков;

- снижение рисков.

Принятие рисков осуществляется в том случае, если уровень рисков признается приемлемым, то есть компания не считает целесообразным применять какие-либо меры по отношению к этим рискам и готова понести ущерб.

Уклонение от рисков – это полное устранение источника риска.

Передача рисков – перенесение ответственности за риск на третьи лица (например, поставщика оборудования или страховую компанию) без устранения источника риска.

Снижение рисков – это выбор и внедрение мер по снижению вероятности нанесения ущерба.

В процессе обработки рисков сначала требуется определить, какие из них требуют дальнейшей обработки, а какие можно принять. Как правило, это решается с помощью оценки приемлемого уровня риска. Риски, равные или ниже приемлемого, можно принять. Очевидно, что для рисков, превышающих приемлемый уровень, требуется выбрать дальнейшие меры по обработке. Приемлемый уровень риска определяется руководством компании или специальной группой, в которую входят руководители и главные финансисты компании. Например, если руководство компании декларирует, что низкий уровень риска считается приемлемым, то дальнейшие действия по обработке рисков определяются только для средних и высоких уровней риска. Причем, средний и высокий уровни риска требуется снизить до низкого (то есть до приемлемого) уровня.

В случае, когда в компании наблюдается большой разброс значений риска (как правило, это может возникнуть, если критичность активов была определена в денежных единицах, а не уровнях), информационные риски можно разбить на категории и определять приемлемый уровень для каждой из них отдельно. Это вызвано тем, что снижать различные значения рисков до одного заданного значения не всегда целесообразно (часто для снижения высоких рисков до заданного уровня необходимы неоправданно большие затраты).

По результатам данного этапа требуется составить «Отчет об обработке информационных рисков компании», который подробно описывает способы обработки рисков. Кроме этого, составляется «План снижения рисков», где четко описываются конкретные меры по снижению рисков, сотрудники, ответственные за выполнение каждого положения плана, сроки выполнения плана.

**Положение о применимости**

По результатам оценки и обработки рисков разрабатывается Положение о применимости. Наличие этого документа обязательно для прохождения сертификации. Положение о применимости содержит все требования приложения А к стандарту ISO 27001 с описанием, выполняются ли данные требования в компании. Если требования не выполняются, необходимо описать причину невыполнения (такой причиной могут быть результаты оценки рисков). Если требования выполняются, следует перечислить документы, которым должно соответствовать их выполнение.

В приложении А к стандарту ISO27001 перечислены все требования к обеспечению безопасности, которые должны выполняться в компании. Следовательно, Положение о применимости является итоговым решением относительно снижения информационных рисков компании.

**Документированные процедуры**

Стандарт требует, чтобы все меры по снижению рисков были документально зафиксированы. То есть для эффективного управления ИБ необходимо наличие процедур, которые будут поддерживаться определенными документами (инструкциями, политиками, регламентами), выполняться определенными людьми. Причем каждая процедура должна быть отражена в соответствующем документе. Документированные процедуры являются обязательным элементом системы управления информационной безопасностью. Следовательно, в рамках системы управления необходимо разработать базу нормативных документов, описывающих все процедуры в области ИБ.

Основными документами по управлению ИБ являются Политика управления информационной безопасностью и Политика информационной безопасности. Политика управления ИБ описывает общий подход к управлению ИБ. Политика ИБ описывает основные процедуры обеспечения ИБ с указанием ссылок на конкретные документы системы управления ИБ.

Кроме этого, разрабатываются методики и инструкции, описывающие процедуры обеспечения ИБ и управления ею.

В качестве примеров можно привести следующие методики:

- Методика инвентаризации активов;

- Методика категорирования активов;

- Методика оценки информационных рисков;

- Методика обработки информационных рисков.

Инструкции следует разработать для каждой процедуры обеспечения информационной безопасности. Примерный перечень может содержать следующие инструкции:

- Инструкция по обеспечению сохранности конфиденциальной информации (соглашение о конфиденциальности);

- Инструкция пользователя по обеспечению информационной безопасности;

- Инструкция системного администратора по обеспечению информационной безопасности;

- Инструкция администратора безопасности;

- Инструкция по управлению доступом пользователей к информационной системе;

- Инструкция по защите от вредоносного программного обеспечения;

- Инструкция по выполнению резервного копирования;

- Инструкция по обращению со съемными носителями информации;

- Инструкция по использованию мобильных компьютеров;

- Инструкция по использованию средств криптографической защиты информации;

- Инструкция по внесению изменений в информационную систему;

- Инструкция по управлению инцидентами информационной безопасности;

- План непрерывности ведения бизнеса;

- Регламент обеспечения физической безопасности.

**Обучение сотрудников компании как способ снижения рисков ИБ**

В настоящей лекции, наверное, нет смысла говорить обо всех способах снижения информационных рисков, поскольку, во-первых, они могут сильно различаться в зависимости от особенностей информационных систем, а, во-вторых, как правило, системные администраторы и администраторы безопасности знают, какие средства защиты требуется внедрить в их информационную систему.

Остановимся подробнее на одном из способов снижения рисков, на который стандарт обращает особое внимание и который часто вызывает сложности при реализации - обучении пользователей информационной системы.

В настоящее время внутренний нарушитель уверено занимает лидирующие позиции среди основных угроз ИБ. Это связано, прежде всего, с тем, что внешний периметр в большинстве компаний защищен достаточно надежно. Кроме этого, сотрудники компании являются легитимными пользователями информационной системы - им необходимо иметь доступ к ценной информации компании для выполнения своих должностных обязанностей. Следовательно, средства защиты в гораздо меньшей степени обеспечивают безопасность информации от внутреннего нарушителя. Основными способами воздействия на сотрудников компании являются нормативные документы, устанавливающие их ответственность за выполняемые действия, и информирование сотрудников по вопросам ИБ. С целью повышения осведомленности сотрудников компании в области ИБ проводятся различные виды тренингов и обучения.

Обучение сотрудников можно выполнять в форме очных и заочных курсов с последующим тестированием. Однако в больших компаниях проведение курсов часто вызывает сложности, так как, во-первых, сложно организовать курсы для большого количества сотрудников, а во-вторых, часто руководителям не хочется отрывать сотрудников от работы для участия в многочасовых семинарах. В таком случае, целесообразно организовать обучение сотрудников с помощью системы дистанционного обучения, в рамках которой могут быть представлены различные курсы (как для пользователей, так и для специалистов), игровые методики обучения, тестирование.

**Управление ИБ**

Управление информационной безопасностью заключается в четком выполнении всех процедур по обеспечению ИБ и по управлению ИБ, координации и регулировании процедур, контроле их правильного, а также эффективного выполнения.

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 на ресурсах, затраченных для достижения целей.

2. Применение РDСА-модели как основы для всех процедур управления ИБ.

РDСА-модель (или модель Шухарта-Деминга) определяет четыре этапа, которые должны выполняться последовательно для каждого процесса.

Таким образом, для каждой процедуры системы управления информационной безопасностью определяются правила выполнения, необходимые ресурсы, график выполнения, процедуры контроля, критерии оценки эффективности. При этом для каждой процедуры последовательно и непрерывно выполняются следующие этапы:

- планирование процедуры;

- внедрение процедуры;

- проверка правильности и эффективности выполнения процедуры;

- внесение необходимых изменений в ход выполнения процедуры.

Далее через определенный период времени требуется заново пересматривать цели и задачи выполнения процедуры, то есть заново приступать к выполнению первого этапа модели РDСА.

Основная сложность может заключаться в проверке эффективности процедур системы управления ИБ. Для каждой процедуры необходимо разработать критерии, по которым будет проверяться ее эффективность, и, кроме этого, такие критерии требуется разработать для всей системы управления в целом.

Критериями оценки эффективности системы управления ИБ могут быть, например, изменение количества инцидентов ИБ, квалификация пользователей в области ИБ и пр.

**Внедрение процедур системы управления ИБ**

Внедрение процедур, как правило, заключается в информировании соответствующих сотрудников о правилах и сроках выполнения процедуры, регулярном контроле выполнения процедуры, а также оценке ее эффективности, внесении корректирующих и превентивных действий, то есть, по сути, во внедрении всего цикла РDСА-модели для каждой процедуры.

Как правило, консультанты по разработке и внедрению системы управления ИБ разрабатывают «План внедрения системы управления», в котором описывают четкую последовательность действий при внедрении процедур, методы контроля и осуществления проверок выполнения процедуры.

**Заключение**

Систему управления ИБ можно считать внедренной и эффективно функционирующей на практике тогда, когда все ее процедуры хотя бы один раз пройдут этапы модели РDСА, когда будут найдены и решены проблемы, возникающие при внедрении процедур.

Обеспечение ИБ и управление ею – достаточно трудоемкие процессы. Однако если к ним подойти комплексно и своевременно, а также выполнять все рекомендации международных стандартов в области управления ИБ - ISO/IЕС 27001:2005 и ISO/IЕС 17799:2005, они станут прозрачными, а защита от угроз безопасности эффективной.