Оглавление

Введение

Одним из основных свойств системы управления информационными услугами является делимость на подсистемы, которая содержит ряд преимуществ с позиций ее разработки и эксплуатации. К таким достоинствам можно отнести упрощение: разработки и модернизации в результате специализации групп проектировщиков по подсистемам; поставки и внедрения типовых подсистем в соответствии с планом выполнения работ; специализации работников в предметной области характерной для соответствующей подсистемы в процессе эксплуатации системы.

Организационная поддержка является одной из важных подсистем, характеризующаяся следующими компонентами (1):

- методические материалы, задающие регламент процесса создания и функционирования системы управления информационными услугами (типовые проектные решения; общеотраслевые руководства; методические материалы по предпроектному обследованию, по созданию и внедрению проектной документации организации).
- средства, для проектирования и поддержки функционирования процесса управления информационными услугами (общесистемные и отраслевые классификаторы, типовые структуры управления предприятием, пакеты прикладных программ, системы документов, и т.п.).
- техническая документация, формирующаяся на этапах обследования, проектирования и внедрения системы управления информационными услугами (обоснование технико-экономических функций и показателей, формирование технического задания, технического проекта и и др. документы).
- требования к персоналу, обеспечивающие функционирование подсистем управления информационными услугами.

Управления информационными услугами невозможно без информационного обеспечения. Информационные услуги основываются на

одной или нескольких информационных подсистемах хранения, обработки и передачи информации. Управление Информационной Безопасностью – важный вид деятельности, целью которого является контроль процессов обеспечения информацией и предотвращение ее несанкционированного использования.

Руководители организации принимают решения по явному или опосредованному управлению информацией, оптимизировать эти процессы возможно при детальном анализе рисков. Этот анализ определит требования к информационной безопасности и будет являться входной информацией для подсистемы Управления Информационной Безопасностью организации.

Требования бизнеса к обеспечению информационной безопасности оказывают воздействие на поставщиков ИТ-услуг и должны быть заложены в нормативных документах организации, в частности в «Соглашениях об Уровне Сервиса». Процесс Управления Информационной Безопасностью заключается в постоянном обеспечении безопасности услуг на согласованном с заказчиком услуг уровне. Безопасность является важнейшим показателем качества менеджмента.

Процесс Управления Информационной Безопасностью заключается в интеграции аспектов безопасности в ИТ-организации с точки зрения поставщика информационных услуг и обеспечивает комплекс документов и мероприятий по разработке, ведению и оценке мер безопасности.

Целью работы является создание типовых решений организации систем управления информационными услугами и информационной безопасностью для организаций различного профиля на примере системы дистанционного обучения

Задачи:

1. Выполнить анализ современных подходов организации систем управления информационными услугами.
2. Выполнить анализ современных подходов организации систем управления информационной безопасностью.

3. Разработать типовое решение управления услугами и оценки риска ИБ на примере системы дистанционного обучения

4. Разработать рекомендации по созданию типовых решений организации систем управления информационными услугами и информационной безопасностью для организаций различного профиля

Глава 1. Процессный подход к управлению ИТ-услугами

1.1 Система управления ИТ-услугами

Традиционный технологический подход, в своей основе, прежде всего, концентрируется на самих технологиях, в основе же IT Service Management(ITSM) подхода управления ИТ-услугами, расположен клиент и его потребности в услугах, предоставляемых с помощью информационных технологий. Причем данный подход сочетает в себе процессную организацию предоставления услуг и зафиксированные в соглашениях об уровне услуг ключевые показатели эффективности (Key Performance Indicators, KPI), что говорит о системности и измеряемости и контролируемости качества предоставления услуги и соответственно управляемости данного процесса.

IT Service Management (ITSM)—управление ИТ-услугами. Внедрение и управление качественными ИТ-услугами, которые соответствуют потребностям бизнеса. Управление ИТ-услугами реализуется поставщиками ИТ-услуг путем использования наиболее оптимального сочетания людей, процессови информационных технологий. (2).

Для информационно-методической поддержки подхода управления ИТ-услугами разработан комплекс документов– IT Infrastructure Library (ITIL) (3). В современной третьей редакции документов ITIL каждый составной элемент комплекса документов ITIL находится в тесной интеграции с другими элементами, что достигается за счет применения подхода Service life cycle– «жизненного цикла сервиса» к ITSM, который заключается в предложенной стратегии сервисов: проектирование сервисов, передача сервисов, эксплуатация сервисов и к постоянное улучшение сервисов. Реализация этого подхода описана в пяти книгах в которых описано управление ИТ сервисами на каждой стадии жизненного цикла:

- Стратегии обслуживания (ServiceStrategies)
- Проектирование услуг (ServiceDesign)
- Внедрение услуг (Service Transition)
- Оказание услуг (Service Operation)
- Непрерывное совершенствование услуг (Continuous Service Improvement).

Функция ServiceDesk неотъемлемый компонент процессной организации подхода ITSM, обеспечивающая одну единую точку входа для запросов всех конечных пользователей и унифицированную процедуру для обработки запросов. Как правило, процессный подход по предоставлению услуг начинает разрабатываться с реализации функции ServiceDesk.

Основу ITSM – составляет совокупность из десяти основных процессов, описанных в томах ServiceSupport и ServiceDelivery библиотеки ITIL:

1. Управление инцидентами (Incident management)
2. Управление проблемами (Problem management)
3. Управление конфигурациями (Configuration management)
4. Управление изменениями (Change management)
5. Управление релизами (Release management)
6. Управление уровнем сервиса (Service Level Management)
7. Управление финансами (Financial management for IT services)
8. Управление доступностью (Availability management).
9. Управление непрерывностью (IT service continuity management)
10. Управление мощностью (Capacity management)

В ITSM определяется множество понятий, на основе которых формируются задачи для отделов, входящих в структуру управления IT (управление конфигурациями, управление инцидентами, управление финансами, управление безопасностью, управление рисками и другие

задачи). Устанавливаются взаимосвязи задач со службами и процессами и даются практические рекомендации по их решению.

В ITSM предлагается выбор структурной модели субъекта рынка ИТ сферы из следующих вариантов:

- инсорсинг – оказание ИТ-услуг силами внутренних специализированных ИТ-подразделений организации;
- аутсорсинг – оказание ИТ-услуг внешней по отношению к организации-субъекту рынка специализированной Сервисной Организацией;
- смешанная модель (ряд сервисов предоставляется внутренним сервисным подразделением организации (инсорсинг), оставшиеся сервисы предоставляются внешними сервисными организациями (аутсорсинг).

Организация должна включать структурный элемент, который является поставщиком услуг IT, который в то же время является и заказчиком для внешних сервисных организаций IT-услуг («служба заказчика»). ITSM содержит описания функций и обязанностей «служба заказчика».

Начиная с версии ISO 20000-1:2011 стандарта “Information technology -- Service management -- Part 1: Service management system requirements» («Информационная технология. Менеджмент услуг») появляются определения ключевых понятий: **service (услуги)** — service management system (система управления услугами) (11).

Услуга (service) — это способ предоставления ценности заказчикам через содействие им в достижении желаемых конечных результатов.

Стандарт ISO 20000-1:2005 не содержал определения центрального понятия — услуги. На то были объяснения: в ITIL v2 тоже, по сути, не было понятия ИТ-услуги, оно в четком виде появилось только в ITIL v3.

Важнейший момент — предоставление заказчикам помощи в достижении их конечных результатов. Это 2/3 определения услуги из ITIL v3. Однако, авторы стандарта не стали включать окончание определения услуги, приведенное в ITIL v3: «.. без принятия ими (заказчиками) на себя специфических затрат и рисков». Это значит, что мировое сообщество еще не

пришло к однозначному выводу, должно ли снижение рисков и специфических затрат фигурировать в определении как обязательный признак услуги. С практической точки зрения определение ITIL v.3 выглядит более интересным, так как позволяет задуматься над тем, как сделать услуги более ценными, и дает направления движения к этой цели. В тоже время, строго говоря, любые способы предоставления ценности (помимо продажи товаров), которые помогают достичь конечных результатов заказчика, считаются услугами. С этим поспорить трудно и стандарт ISO 20000-1:2011 в этом прав.

В стандарте нет определения функции. Функции существовали всегда и они также несли ценность, но при выполнении функции сотрудники не думают, как улучшить предоставление функции и сделать ее более ценной. При выполнении функции действует принцип — выполнить в рамках регламента. Понятие услуги предполагает не просто помощь в чем-то, но и при этом включает в себя понимание заказчика и его желаемых результатов. В стандарте понятия «функция» нет, возможно из за того, что в «западном» менталитете понятие функция уже давно заменено понятием услуга.

Система управления услугами (Service management system - SMS) — это система управления, направляющая и контролирующая действия по управлению услугами сервис-провайдера.

Причем четко разделяются понятия система управления услугами, процессы управления услугами и сами услуги (рисунок 1.1) Важно различать, что система управления услугами — это следующий уровень управления, расположенный выше процессов администрирования и управления технологическими компонентами ИТ-инфраструктуры. Это отдельная группа процессов, как операционных, так и тактических которые определяют, как будут управляться услуги и как сделать эти услуги надежными, качественными и предсказуемыми.

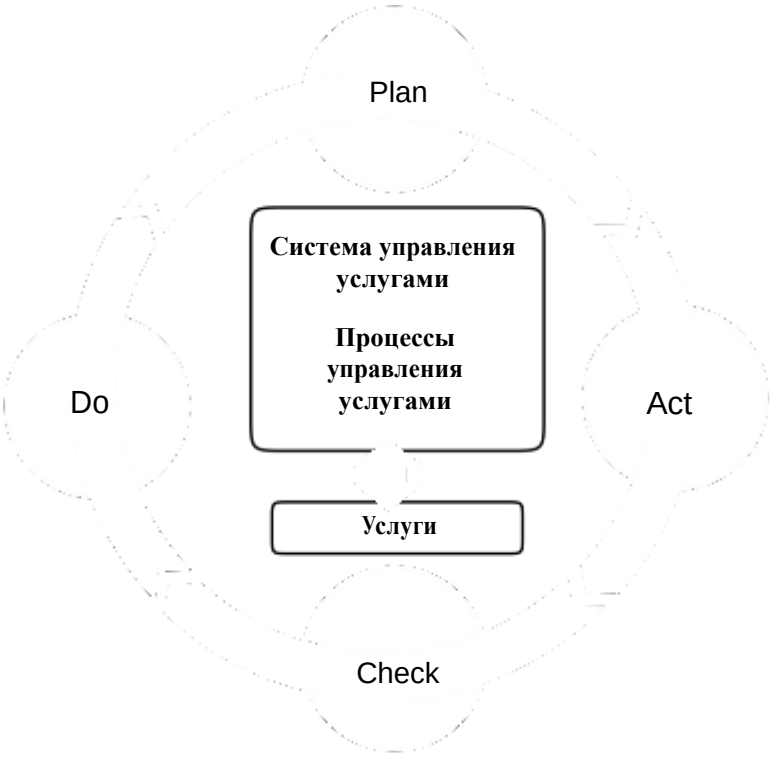


Рис 1.1. Система управления услугами в ISO 20000-1:2011.

Plan (Планирование системы управления услугами)

Планы управления услугами должны, как минимум, определять:

- известные ограничения, которые могут влиять на систему управления услугами;
- требования к услугам;
- цели управления услугами, которые должны быть достигнуты сервис-провайдером;
- структура полномочий, ответственности и процессных ролей;
- политики, стандарты, регуляторные требования и контрактные обязательства;
- полномочия и ответственность за планы, процессы управления услугами и услуги;
- подход, применяемый для работы с другими сторонами, вовлеченными в разработку и преобразование сервисных процессов
- люди, технические, информационные и финансовые ресурсы, необходимые для достижения целей управления услугами;

- подход, применяемый для взаимодействия между процессами управления услугами и другими компонентами системы управления услугами;
- технологии для поддержки системы управления услугами;
- подход, применяемый для управления рисками и критерии принятия рисков;
- способы измерения, аудита, отчетности по эффективности системы управления услугами.

Act (Поддержка и улучшение системы управления услугами)

Должна быть разработана политика непрерывного совершенствования услуг. Провайдер услуг должен управлять улучшениями, включая:

- получения уверенности, что одобренные улучшения внедрены;
- постановку целей улучшений в направлениях качества, ценности, возможностей, стоимости, производительности, использования ресурсов и уменьшения рисков;
- пересмотр политик управления услугами, планов, процессов и процедур, когда это необходимо;
- отчетность о внедренных улучшениях;
- измерение внедренных усовершенствований по отношению к установленным целям, если цели не достигнуты обсуждение необходимых действий.

DO (Внедрение и функционирование системы управления услугами)

Сервис-провайдер должен внедрить систему управления услугами, включая:

- распределение полномочий, ответственности и процессных ролей;
- распределение и управление фондами и бюджетами;
- управление человеческими, техническими и информационными ресурсами;

- управление процессами управления услугами;
- идентификацию, оценку и управление рисками, связанными с услугами;
- мониторинг и отчетность о производительности деятельности в области управления услугами.

Check (Мониторинг и анализ системы управления услугами)

Провайдер услуг должен применять подходящие методы, для мониторинга измерения системы управления услугами и самих услуг. Они должны включать внутренние аудиты и проверку руководством. Внутренние аудиты должны определять, что система управления услугами:

- соответствуют требованиям настоящего стандарта;
- эффективно выполняются и поддерживаются. Проверка руководством должна включать как минимум: а) обратную связь от пользователей;
- соответствуют сервисным требованиям и требования к системе управления услугами идентифицированы;
- производительности и согласованность услуг и процессов;
- текущие и будущие человеческие и технические возможности;
- текущие и будущие человеческие, технические, информационные и финансовые ресурсы;
- риски;
- статус превентивных и корректирующих мер;
- результаты аудитов и проверок качества управления и последующие действия;
- изменения, которые могут влиять на систему управления услугами и сами услуги;
- возможности для улучшения.

Предоставление услуг несет ценность, путем улучшения результатов которые заказчик хочет достичь. И строго говоря, предоставление услуг должно снижать риски и уменьшать специфические затраты. Но, всегда ли

услуги снижают риски и стоимость или нет, тут очевидно, нет единого мнения. Простой пример, я выполнил за кого-то определенную простую работу. Услуга оказана, я помог заказчику достичь результата. Однако, взял ли я на себя риски и снизил ли по стоимости взяв на себя специфические затраты — это вопрос. Есть весьма простые, технические услуги, не ведущие ни к развитию, ни к инновациям. И они могут выполняться совсем не дешевле и не менее рискованно. Вполне возможно, в этом случае провайдер не специализируется на этом виде деятельности, ведь если бы он специализировался, то услуга была бы оказана дешевле, надежнее и т.д. Но всегда ли так происходит? Строго говоря, с точки зрения стандарта, если услуги выполняются ни дешевле, ни менее рискованно, это, тем не менее, можно считать услугой.

Система управления услугами должна состоять из следующих элементов:

1. **«Ответственность топ-менеджмента»** и этот раздел в стандарте ISO 20000-1:2011 существенно расширен. Это стыковка со стандартом ISO 9000 — именно топ- менеджмент должен взять на себя ответственность за управление качеством и обеспечить это в своей компании. Появились требования к топ-менеджменту в отношении политики управления услугами, а также к представителю топ-менеджмента в управлении сервис-провайдером.

2. **«Руководство процессами, которые выполняются другими сторонами»**.

3. **«Управление документами»**.

4. **«Управление ресурсами»**, которые подразделяются на людские, технические, информационные и финансовые. Вынося управление ресурсами на самый верх- ний уровень системы управления, авторы утверждают, что это важнейший элемент системы, необходимое условие решения задачи управления.

5. Использование цикла PDCA для постоянного улучшения системы управления услугами.

Стандарт ISO 20000-1:2011 четко определяет использование цикла PDCA для постоянного улучшения системы управления услугами. В отличие от аналогичного подхода ISO

20000-1:2005 в стандарте 2011 года основные требования существенно переформулированы и гораздо более отточены и четки. Поэтому мы приведем их на рис. 1.2.

Рисунок 1.2. Использование цикла PDCA для постоянного улучшения системы управления услугами

Отметим, что в стандарт введена важнейшая функция — внутренний аудит (контроль). Такая функция крайне полезна. Это сближает стандарт с

COBIT, требованиями Basel II и других стандартов. Заметим, что речь идет именно о внутреннем аудите (контроле), который делается либо самими членами команды менеджеров, либо специальным подразделением внутри компании. К сожалению, в России существует устойчивое понимание аудита именно как внешнего, осуществляемого внешней компанией. Однако мировая практика напротив, наибольшее значение придает внутреннему контролю. Такой контроль можно рассматривать как первую ступень аудита, когда инструменты и методы внутреннего контроля использует сам руководитель, для того чтобы контролировать как работает система управления услугами. Внутренний контроль, выполняемый специализированным внутренним подразделением, можно рассматривать как вторую ступень аудита, а уже всем привычный внешний аудит — как третью.

ITIL (Information Technology Infrastructure Library) предлагает смотреть на деятельность ИТ-подразделения с позиции того что оно формирует прибавочное качество, как и остальные подразделения организации. Причем ИТ-подразделение теперь не предоставляет в пользование оборудование, а предоставляет ИТ-услуги, необходимые для конечных пользователей, которых в таком контексте предпочтительнее именовать «потребителями услуг». Можно сказать, что предоставляемое оборудование «обертывается» услугами по его поддержке и предоставлению. Переход на термин ИТ-услуги требует перехода от отношений владелец-пользователь оборудования (приложений) к отношениям покупатель-продавец ИТ-услуг, что в свою очередь требует выработки способов измерения качества предоставляемых услуг. Помимо этого вводится понятие стоимости услуги, что фактически выводит ИТ-подразделение на финансовое взаимодействие между ИТ-подразделением и бизнесом. Фактически библиотека ITIL предлагает построение процессной модели для управления ИТ-подразделением, результатом деятельности которого являются ИТ-услуги для бизнеса с прозрачной стоимостью, качество которых гарантируется путем организации непрерывного контроля. Библиотека ITIL содержит лучший мировой опыт по

построению единой комплексной системы управления ИТ-подразделением, который возможно применять к конкретной ситуации.

Поскольку библиотека является свободно распространяемой, то она является наиболее применяемым сегодня подходом к управлению ИТ-услугами, который применим ко всем секторам и организациями любого размера. ITIL может быть внедрен как полностью, так и частично, и фактически, это некоторая система взглядов на управление информационными технологиями в компании. Владельцем проекта ITIL в настоящее время является OGC/CCTA (Офис правительственной коммерции /Центральное агентство по компьютерам и телекоммуникациям). Обобщение опыта управления ИТ на протяжении 20 лет под эгидой правительства Великобритании сделало книги ITIL по всем основным областям управления ИТ стандартом «де-факто».

1.2 Применение процессного подхода к реализации процессов управления услугами и информационной безопасностью

Необходимо выстраивать управление службой ИБ на основе процессного подхода, при условии, что эта служба состоит более чем из одного-двух сотрудников. Служба ИБ должна быть встроена в процессы управления и интегрирована с ними. В свою очередь, руководителю, отвечающему за ИБ, необходимо участвовать в процессах, происходящих в организации, иногда даже возглавляя их, если это необходимо для обеспечения информационной на всех этапах, начиная от разработки и заканчивая внедрением и последующим выводом из эксплуатации и уничтожением тех или иных процессов и систем. Необходимо не только смотреть на свой участок работы, но и понимать архитектуру решений и бизнес-требования, а также влиять на них, если видишь, что решение может быть неверным или неоптимальным (7).

Ориентация подразделения ИБ на предоставление бизнесу качественных услуг по управлению рисками ИБ, обеспечение соответствия требованиям по ИБ и организации процессов ИБ является важной частью подхода к корпоративному управлению и интеграции функции информационной безопасности в общую структуру бизнеса компании. Для бизнес-подразделений информационная безопасность становится одной из важных потребляемых услуг, направленной на повышение надежности и безопасности бизнеса и снижение различных издержек, связанных с рисками ИБ. При этом защита информационных активов компании, владельцами которых являются бизнес-подразделения, становится услугой, предоставляемой им подразделением ИБ (7).

В сервисной модели предоставления услуг все сервисы описаны, детализированы, для каждого сервиса имеются свои метрики, за каждым сотрудником службы информационной безопасности закреплены роль и определена доля участия в определенном сервисе, рассчитаны себестоимость сервисов и тарифы, определены KPI, с помощью которых можно отслеживать соответствие сервиса закрепленному в SLA уровню (7).

Результатом деятельности подразделения ИБ не может быть набор услуг, так как оказываемые подразделением услуги в результате направлены на защиту активов организации, на предотвращение финансового и репутационного ущерба, поэтому для бизнес-подразделений важна разумная уверенность в том, что уровень рисков ИБ приемлем для бизнеса. А если рассматривать с точки зрения сервисной модели предоставления услуг, то результатом деятельности службы ИБ является выполнение зафиксированного в SLA уровня сервиса (7).

Безопасность — это постоянный процесс, а процесс как раз и требует постоянного или периодического выполнения определенных действий, которые можно реализовывать в виде услуги ИБ. Среди подобных услуг могут быть и те, что предоставляются внутренними подразделениями, и

услуги от внешних поставщиков. Каким образом распределить, что и кому доверить, — это зависит от модели угроз конкретных предприятий (7).

Методики, что используются в ИТ-службах (например, ITIL/ITSM) достаточно абстрактны, но дают возможность использовать их в любой сфере деятельности ИТ в том числе могут применяться в службах ИБ.

В сфере ИБ есть свои требования и стандарты, такие как ISO 27001, 27002, 27005, 17799, PCI DSS, СТО БР и другие. Эти документы так или иначе пересекаются и дополняют друг друга».

К услугам ИБ, как и к другим услугам, связанным с ИТ, могут быть успешно применены рекомендации ITSM — например, по управлению уровнем услуги и мониторингу основных ее параметров, формализация которых производится при заключении SLA с бизнес-подразделениями. Для услуги ИБ такими параметрами являются обеспечение конфиденциальности, целостности и доступности. Для реализации комплексной системы управления информационной безопасностью в соответствии с лучшими практиками управления ИБ, изложенными в стандартах серии ISO 27000, необходимо использовать цикл Деминга и процессный подход (7).

При определении списка процессов, которые в службе ИБ следует выстроить в первую очередь, необходимо исходить из результатов анализа рисков ИБ в конкретной организации. Обычно наиболее критичны процессы управления правами доступа, обеспечения конфиденциальности и управления инцидентами ИБ. Это базис, на основе которого необходимо в целом выстраивать процесс обеспечения ИБ. Естественно, нужна и детализация процессов внутри службы, чтобы понимать, какие из них низкоэффективны, какие требуют больших трудозатрат при небольшой отдаче, какие основаны на выполнении рутинных операций и требуют автоматизации. Если мы в дальнейшем заботимся о повышении качества и снижении стоимости сервиса, то разрабатываем план оптимизации процессов от каких-то отказываемся, какие-то отдаем на аутсорсинг, какие-то автоматизируем (7).

К наиболее критичным процессам относятся «управление доступом, управление рисками ИБ, анализ эффективности ИБ, аудит процессов ИБ, обеспечение непрерывности ИТ-сервисов и резервное копирование, а также управление инцидентами ИБ» (7).

Все эти процессы требуют формализации, детального описания и вовлечения сотрудников различных подразделений, процессный подход позволяет организовать передачу отдельных процессов ИБ на аутсорсинг, поскольку дает возможность четко разграничить ответственность сторон, опираясь на формализованную модель процесса с указанием его входов, выходов, необходимых ресурсов, документации и связей с другими процессами управления ИБ и ИТ» (7).

Не следует забывать о процессе регулярной профессиональной переподготовке служб ИБ (чтобы они не теряли адекватности в анализе ситуации и профессионально реагировали на инциденты — так как сейчас вопрос обычно состоит не в том, произойдет ли инцидент, а в том, когда это будет и насколько оперативно и грамотно на него среагирует компания) и о повышении знаний об ИБ у обычных пользователей.

Применение процессного подхода к реализации процессов управления ИТ и ИБ позволяет выстроить интегрированную систему управления ИТ-рисками, объединяющую в себе процессы управления рисками ИБ (в соответствии с ISO 27000), рисками управления ИТ-сервисами (на основе ISO 20000 и ITIL) и рисками прерывания бизнеса (по стандартам BS 25999, BS 25777 и ISO 22301). Создаваемая таким образом в соответствии с лучшими практиками, описанными в ISO 31000, интегрированная система управления рисками представляет собой синергию систем управления и дает возможность объединить схожие процессы систем управления рисками, снизить затраты на их операционную поддержку и повысить эффективность управления рисками благодаря предотвращению дублирования операций и комплексному подходу к рассмотрению ИТ-рисков применительно к

поддерживаемым ИТ бизнес-процессам, влияющим на бизнес компании в целом (7).

Компаниям и службам информационной безопасности полезно иметь каталог услуг ИБ. Каталог услуг может иметь многоуровневую структуру. В двухуровневом каталоге сервисов ИБ Первый уровень определяет оказываемый сервис, второй уровень разбивает его на отдельные услуги. Целиком сервис может быть не слишком интересен бизнес-подразделениям, но отдельные услуги, входящие в него, чрезвычайно востребованы.

Как видим, процессный подход позволяет гармонично строить деятельность служб ИБ. Очень важно, чтобы этот процесс соответствовал ключевым принципам, на которых строится процессное управление организацией в целом. Итогом этих усилий станет гораздо более четкая и понятная бизнесу работа, нацеленная на результат, который можно измерить по заранее согласованным показателям.

1.3 Процессный подход к управлению организацией в системе базовых приоритетов всеобщего управления качеством

Понятие «процессный подход» в системе базовых приоритетов всеобщего управления качеством часто употребляется руководителями и специалистами организаций. Но однозначного определения «классического» процессного подхода, так же как и определения «процесса», на сегодняшний день нет.

В дальнейшем будет использоваться следующее понятие бизнес-процесса: «Бизнес-процесс — совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующая «входы» в «выходы», представляющие ценность для потребителя» (9 стр. 356).

Это определение близко к определению стандарта ISO серии 9001:2008, но не отражает, где именно локализована деятельность, преобразующая входы в выходы. Это может быть деятельность, выполняемая

в рамках одного структурного подразделения или отдела, а может быть деятельность, выполняемая различными подразделениями.

Для определения элементов процесса часто используют понятие «5М» (рисунок 1.3).

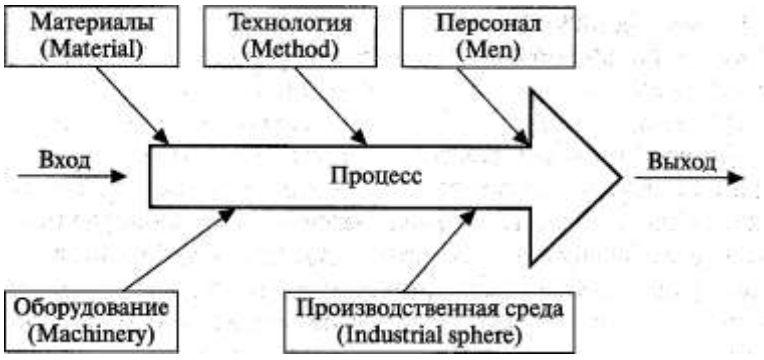


Рисунок 1.3. Пять составляющих процесса (5М)

Для более подробной декомпозиции процесс можно расчленить на 12 элементов:

1) технология;
2) персонал;
3) оборудование;
4) оснастка и инструменты;
5) контрольно-измерительное и испытательное оборудование;
6) нормативная документация;
7) основные материалы;
8) вспомогательные материалы;
9) производственная среда;
10) теплоэнергоносители;
11) программное обеспечение;
12) информация.

Этот список можно варьировать. Однако с точки зрения процессного подхода к управлению организацией большее применение имеет другое

представление элементов процесса (рисунок 1.4),

Рис. 1.4. Элементы процесса

- выходы бизнес-процесса;
- входы бизнес-процесса;
- ресурсы;

•клиенты;

- владелец бизнес-процесса;
- информация о процессе.

Вход бизнес-процесса — материальный или информационный объект, который в ходе выполнения процесса преобразуется в выход.

Выход бизнес-процесса — материальный или информационный объект, являющийся результатом выполнения процесса и потребляемый внешними по отношению к процессу клиентами (другими процессами или субъектами). Результат выполнения процесса может использоваться в качестве ресурса при выполнении другого процесса.

Ресурс бизнес-процесса — материальный или информационный объект, постоянно используемый для выполнения процесса, но не являющийся входом процесса. К ресурсам процесса относятся: информация, персонал, оборудование, программное обеспечение, инфраструктура, среда, транспорт и пр. Ресурсами процесса управляет владелец процесса.

Клиент (потребитель) — субъект, получающий результат бизнес-

процесса.

Внутренний клиент находится в организации и в ходе своей деятельности использует результаты предыдущего бизнес-процесса.

Внешний клиент находится за пределами организации и использует результат (выход) бизнес-процесса.

Владелец процесса — должностное лицо, имеющее в своем распоряжении ресурсы; осуществляет мониторинг хода процесса и управление ходом процесса, несет ответственность за результат и эффективность процесса.

В роли владельца процесса может выступать коллегиальный орган управления. Ответственность за результат и эффективность процесса владелец несет перед вышестоящим руководителем или собственником (представителем собственника, собранием акционеров).

Управление процессом ведется путем планирования и перераспределения ресурсов.

Функция — совокупность однородных операций, выполняемых структурным подразделением на постоянной основе.

Регламент бизнес-процесса — документ, описывающий последовательность операций, ответственность, порядок взаимодействия исполнителей и порядок принятия решений по улучшениям.

Формат описания бизнес-процесса (нотация) — способ представления графической модели бизнес-процесса.

Определить бизнес-процесс как объект для управления означает:

- назначить владельца процесса;
- определить клиентов и выходы (результаты) процесса;
- разработать систему управления процессом (цели управления, показатели процесса, систему отчетности и пр.);
- определить поставщиков и входы процесса;

- выделить владельцу процесса ресурсы, необходимые для выполнения процесса и управления им (инфраструктура, оборудование, персонал, информация и т.д.);
- разработать регламенты выполнения процесса.

Выделяют основные и вспомогательные процессы

Основной (первичный) процесс — это процесс текущей деятельности организации, добавляющий ценность продукции или услуге. К основным процессам относятся процессы производства, сбыта, снабжения и др.

Вспомогательный (поддерживающий) процесс — это процесс, не создающий добавленную ценность. Вспомогательные процессы необходимы для обеспечения основных процессов. Как правило, вспомогательный процесс поставляет ресурсы для основных процессов и увеличивает стоимость продукции или услуги.

Перечень основных бизнес-процессов по этапам жизненного цикла, изложенный в стандарте ISO 9004-1:1994 на основе жизненного цикла продукции:

- Маркетинг и изучение рынка
- Проектирование и разработка продукции
- Проектирование и разработка процессов
- Закупки
- Производство
- Проверки
- Упаковка и хранение
- Установка и распределение
- Установка и ввод в эксплуатацию
- Техническая помощь и обслуживание
- Послепродажная деятельность
- Утилизация и переработка в конце полезного срока службы.

1.4 Система показателей и регламентация бизнес-процесса

Для построения системы управления процессом необходимо иметь плановую и оперативную информацию о нем. Потребители этой информации — владелец процесса и руководитель организации.

Задачи измерения показателей процесса следующие:

- получение данных для мониторинга процесса, установления несоответствий и своевременного принятия корректирующих и предупреждающих мероприятий;
- получение данных, необходимых для управления процессом и проведения его диагностики на основе фактов, а не догадок;
- определение характеристик качества процесса и его результатов;
- установление проблем, связанных с обеспечением качества, на ранних этапах и предупреждение их в дальнейшем;
- обеспечение ответственности исполнителей за результаты своей работы.

Показатели процесса делятся на две группы — показатели производительности и показатели эффективности.

Эффективность показывает, насколько результаты процесса удовлетворяют клиентов (измеряется после выполнения процесса).

Производительность характеризует, насколько процесс соответствует внутренним требованиям организации (измеряется до начала выполнения процесса и в ходе его выполнения)

При отборе показателей, как правило, принимают во внимание:

- какие показатели позволяют иметь лучшее представление о качестве результатов процесса;
- какие показатели позволяют лучше оценить реакцию потребителей;
- насколько показатели отражают реальное положение дел, есть ли другие показатели, у каких показателей наивысший приоритет;

- можно ли получить необходимую информацию внутри организации; если невозможно, то каким образом можно оценить процесс;

Глава 2. Сущность управления информационной безопасностью

Управление Информационной Безопасностью является аспектом обеспечения общей информационной безопасности, по обеспечению сохранности информации. Под сохранностью понимается защищенность от известных рисков, а также отслеживание и реагирование на неизвестные, в том числе появляющиеся новые риски. Ценность информации оказывает непосредственное влияние на требуемый уровень конфиденциальности, целостности и доступности.

- Конфиденциальность – защита информации от несанкционированного доступа и использования.
- Целостность – полнота, точность, своевременность информации.
- Доступность – обеспечение доступа к информации в рамках согласованного периода времени.

Дополнительные аспекты обеспечивают приватность (целостность и конфиденциальность частной информации), анонимность и проверяемость (проверка использования информации по назначению и результативности мероприятий по обеспечению безопасности).

Увеличивающееся влияние ИТ-инфраструктуры в процессах обеспечения функционирования организации, свидетельствует о росте уязвимостей и сбоев в работе программно-технических средств, человеческих ошибок, действий злоумышленников, хакеров, компьютерных вирусов и др. Такое усложнение, в силу увеличивающегося количества возможных инцидентов в обеспечении информационной безопасности, требует унифицированного подхода к реализации управленческих решений. Процесс управления информационной безопасностью тесно связан с другими процессами и в ряде случаев определённые виды деятельности по обеспечению информационной безопасности выполняются другими процессами, описанными в библиотеке ITIL.

Процесс управления информационной безопасностью содержит два

компонента:

- выполнение требований безопасности, закрепленных в соглашении об уровне предоставления услуги – Service Level Agreement (SLA) и других требованиях включающих внешние договоры, законодательные акты и установленные правила;

- обеспечение базового Уровня Безопасности, в независимости от внешних требований.

Многие современные организации обеспечивают информационную безопасность либо на стратегическом уровне, что находит отражение в информационной политике и информационном планировании, либо на операционном уровне, подразумевающим закупку средств обеспечения информационной безопасности. Как правило, во многих организациях, недостаточно внимания уделяется вопросам непосредственного управления информационной безопасностью, регулярному анализу и совершенствованию требований и технических решений.

Разрыв между операционным и стратегическим уровнями приводит к тому, что на тактическом уровне большие средства вкладываются в неактуальные меры безопасности, когда уже необходимо принимать новые, более эффективные меры.

Поэтому процесс Управления Информационной Безопасностью должен обеспечивать поддержку принятия эффективных решений по обеспечению информационной безопасности на всех уровнях стратегическом, тактическом и операционном.

Меры по обеспечению информационной безопасности должны соответствовать уровню важности информации. Должен соблюдаться баланс между тремя компонентами: меры безопасности, ценность информации, существующие угрозы информационной безопасности организации.

2.1 Взаимосвязь управления информационной безопасностью с другими процессами

Управление информационной безопасностью сводится к регулярным повторяющимся действиям: планированию, выполнению процедур обеспечения информационной безопасности, подготовка и осуществление проверок, составление актов.

Виды деятельности по управлению информационной безопасностью по материалам открытого геопространственного консорциума Open Geospatial Consortium (OGC) представлены на рисунок 2.1.

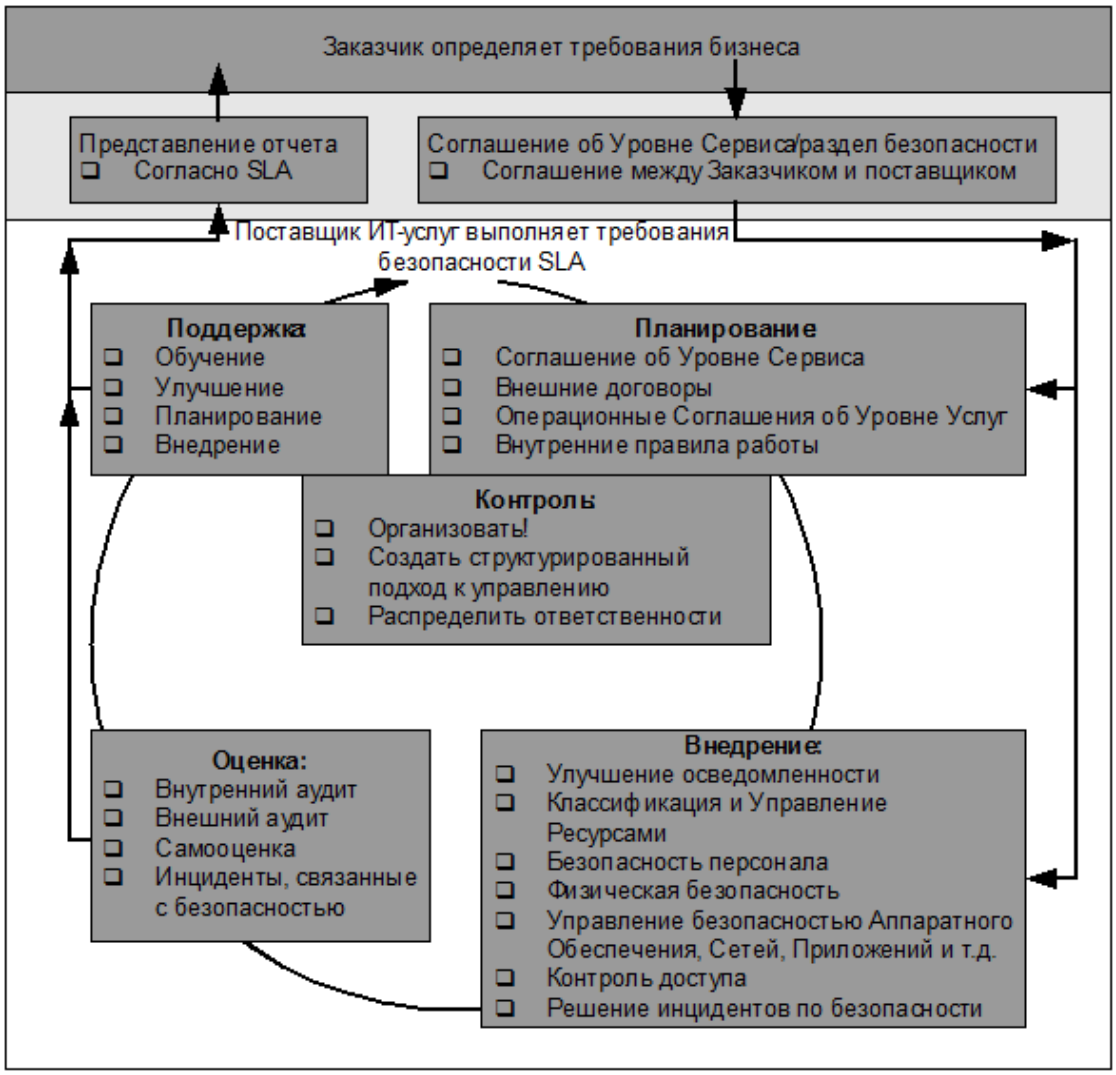


Рисунок 2.1. Виды деятельности по управлению информационной безопасностью

Входными данными процесса служат требования заказчика, представленные в разделе безопасности под названием «Соглашения об Уровне Сервиса» Требования сформулированы как услуги по безопасности обеспечивающие необходимый уровень безопасности.

Поставщик услуг на основе «Соглашения об Уровне Сервиса» составляет план по безопасности ИТ-организации, в котором отражены критерии безопасности организации. Полученный план согласовывается, оценивается, корректируется и утверждается у заказчика. В результате чего и заказчик и поставщик информационных услуг совместно формируют жизненный цикл процесса.

Процесс Управления Информационной Безопасностью по представлению OGC связан с другими процессами ITIL (см. рисунок 2.2), по причине того что другие процессы содержат действия, связанные с обеспечением информационной безопасности. Эта действия проводятся в плановом порядке с учетом зоны ответственности определенного процесса и его руководителей. Процесс же «Управления Информационной Безопасностью» обеспечивает другие процессы общими инструкциями о структуре деятельности, относящейся к области информационной безопасности.

Рисунок 2.2 Взаимосвязь «Процесса Управления Информационной безопасностью» и других процессов

Управление Конфигурациями

Для обеспечения информационной безопасности процесс «Управления конфигурациями» наиболее значим, из за того, что он позволяет классифицировать «Конфигурационные Единицы» (configuration item, CI) представляющие собой активы, компоненты сервиса или другие элементы, которые находятся или будут находиться под контролем процесса управления конфигурациями. На основе этой классификации определяются связи между «Конфигурационными Единицами» и процедурами обеспечения информационной безопасности.

ИТ-организация для каждого Уровня Классификации должна осуществлять комплекс мер информационной безопасности. Эти комплексы описываются как процедуры. Например "Процедура взаимодействия сотрудника организации с носителями данных содержащих личную информацию".

Классификация это ключевой момент обеспечения информационной безопасности. Поэтому каждую «Конфигурационную Единицу» в «Конфигурационной Базе Данных» (Configuration Management Data Base - CMDB) необходимо классифицировать. Таким образом, классификация является связующим звеном между Конфигурационной Единицей и

соответствующим комплексом мер безопасности.

Управление Инцидентами

Рекомендуется в соглашения SLA включать определение типов инцидентов по безопасности. Каждый инцидент, оказывающий препятствие в достижении базового внутреннего «Уровня Безопасности», должен классифицироваться как инцидент по безопасности.

Сообщения об инцидентах поступают как от пользователей, так и от различных «Процессов Управления». Важно, чтобы «Процесс Управления Инцидентами» определял все инциденты по безопасности. Это требуется для вызова процедур для обработки соответствующих инцидентов. Руководителю Процесса Управления Информационной Безопасностью, желательно быть в курсе всех внешних сообщения, относящиеся к инцидентам по безопасности.

Управление Проблемами

Процесс Управления Проблемами идентифицирует и устраняет структурные сбои по безопасности. В случае возникновения риска для системы безопасности процесс «Управление Проблемами» должен вызвать «Процесс Управления Информационной Безопасностью». Принятое решение по устранению проблем информационной безопасности должно быть проверено и быть основано на согласованности предлагаемых вариантов решений с внутренним требованиям безопасности и требованиями соглашений SLA.

Управление Изменениями

По достижению приемлемого уровня безопасности, находящегося под контролем «Процесса Управления Изменениями», процесс «Управления изменениями» гарантирует, что этот уровень безопасности будет обеспечиваться также после произошедших изменений. Для этого используются определенные стандартные операции. Каждый запрос на изменение (RFC) содержит ряд параметров, которые учитываются процедурой приемки. Так параметры степени воздействия и срочности могут

дополняться параметром, связанным с безопасностью. При оказании Запросом на изменения (RFC) значительного воздействия на информационную безопасность, будут осуществляться расширенные приемочные испытания и процедуры.

Запрос на изменения (RFC) должен содержать предложения по решению вопросов безопасности, которые должны быть основаны на базовом уровне внутренней безопасности организации и требованиях SLA. Каждую мера безопасности, связанную с внесением изменений, необходимо реализовывать в то же время, что и проведением самих изменений, а также необходимо проводить совместное тестирование внедренных решений. Тесты по безопасности имеют более сложную структуру, чем обычные функциональные тесты. Обычные тесты определяют доступность определенных функций. Тесты же по безопасности проверяют помимо доступности функций безопасности, и отсутствие других, функций, влияние которых может снизить безопасность системы.

Процесс «Управление изменениями» добавляет новые меры обеспечения безопасности в ИТ-инфраструктуру в соответствии с изменениями этой инфраструктуры.

Управление Релизами

Процесс «Управления Релизами» выполняет контроль и обновление до новых версий программного и аппаратного обеспечения. Он гарантирует:

- использование соответствующего аппаратного и программного обеспечения;

- тестирование перед использованием аппаратного и программного обеспечения;

- санкционирование внедрения с помощью процедуры изменения;

- легальности программного обеспечения;

- защиту программного обеспечения от вирусов;

- регистрацию номеров версий в Базе Данных CMDB процесса «Управления Конфигурациями»;

- оптимальности процесса установки.

В этом процессе подразумевается использование обычной процедуры приемки, которая должна включать аспекты информационной безопасности. Рассмотрение аспектов безопасности в является особенно важным. Это означает, что

Требования и меры по безопасности, которые определены определенные в SLA, должны постоянно соблюдаться, в том числе в ходе тестирования и приемки.

Управление Уровнем Сервиса

Процесс «Управления Уровнем Сервиса» обеспечивает гарантии договоренности об услугах, которые предоставляются заказчикам, четко определены и выполняются. В соглашениях об «Уровне Сервиса» так же необходимо учитывать меры по обеспечению безопасности, это приводит к оптимизации уровня предоставляемых услуг. Управление «Уровнем Сервиса» содержит виды деятельности, непосредственно связанных с безопасностью, в которых важное значение принадлежит «Управлению Информационной Безопасностью»:

1. Потребности заказчика по обеспечению безопасности.

2. Анализ осуществимости требований заказчика по обеспечению безопасности.

3. Предложение, определение и обсуждение уровня безопасности ИТ-услуг в SLA.

4. Определение, разработка и формулирование системы внутренних требований безопасности для ИТ-услуг.

5. Мониторинг изменений стандартов безопасности (OLA).

6. Составление и предоставление отчетов о всех предоставляемых услугах.

«Управление Информационной Безопасностью» предоставляет для «Управления Уровнем Сервиса» необходимую входную информацию и обеспечивает поддержку для выполнения перечисленных выше видов

деятельности с 1 по 3. Виды деятельности относящиеся к пунктам 4 и 5 проводятся «Управлением Информационной Безопасностью». Для вида деятельности под номером 6 и другие все процессы, включая и «Управление Информационной Безопасностью» предоставляют требуемую входную информацию. В ходе составления соглашений SLA, как правило, предполагается, что необходимо обеспечить общий базовый Уровень Безопасности (baseline). Дополнительные требования заказчика по вопросам обеспечения безопасности должны четко определяться в SLA.

Управление Доступностью

Процесс Управления Доступностью подразумевает обеспечение технической доступности ИТ-компонентов, связанной с доступностью услуги. Уровень качества доступности характеризуется непрерывностью, устойчивостью и восстанавливаемостью.

Важным является организация взаимодействия между Процессами Управления Непрерывностью ИТ-услуг, Управления Доступностью и Управления Информационной Безопасностью, потому что большинство мер по обеспечению безопасности оказывают положительное воздействие как на доступность, так и на важные аспекты безопасности — и целостность и конфиденциальность.

Управление Мощностями

«Процесс Управления Мощностями» следит за наилучшим использованием ИТ-ресурсов в определенной договоренности с заказчиком. Большинство видов деятельности «Процесса Управления Мощностями» влияет на доступность, поэтому и на «Процесс Управления Информационной Безопасностью».

Управление Непрерывностью ИТ-услуг

Процесс «Управления Непрерывностью ИТ-услуг» гарантирует, что влияние непредвиденных обстоятельств будет ограничено ранее определенным уровнем, требований заказчика, так, что чрезвычайные обстоятельства не должны приводить к краху деятельности организации.

Ключевыми видами деятельности являются поддержка, определение, внедрение и тестирование плана обеспечения непрерывной работы и восстановления функционирования, а также принятие превентивных мер. Присутствие в этих видах деятельности аспектов безопасности обеспечивает связь с Процессом Управления Информационной Безопасностью. Напротив, невозможность выполнения базовых требований безопасности может рассматриваться как чрезвычайное обстоятельство.

2.2 Раздел по Безопасности Соглашения об Уровне Сервиса

Соглашение об Уровне Сервиса (SLA) определяет договоренности с заказчиком. Процесс Управления Уровнем Сервиса отвечает за соглашения SLA (см. также главу 10). Соглашение SLA является главной движущей силой всех процессов ITIL.

ИТ-организация определяет степень выполнения требований SLA, включая требования по безопасности. Определенные в SLA элементы безопасности должны отвечать соответствующим потребностям заказчика. Заказчик должен определить важность всех бизнес-процессов (см. рисунок 2.3).

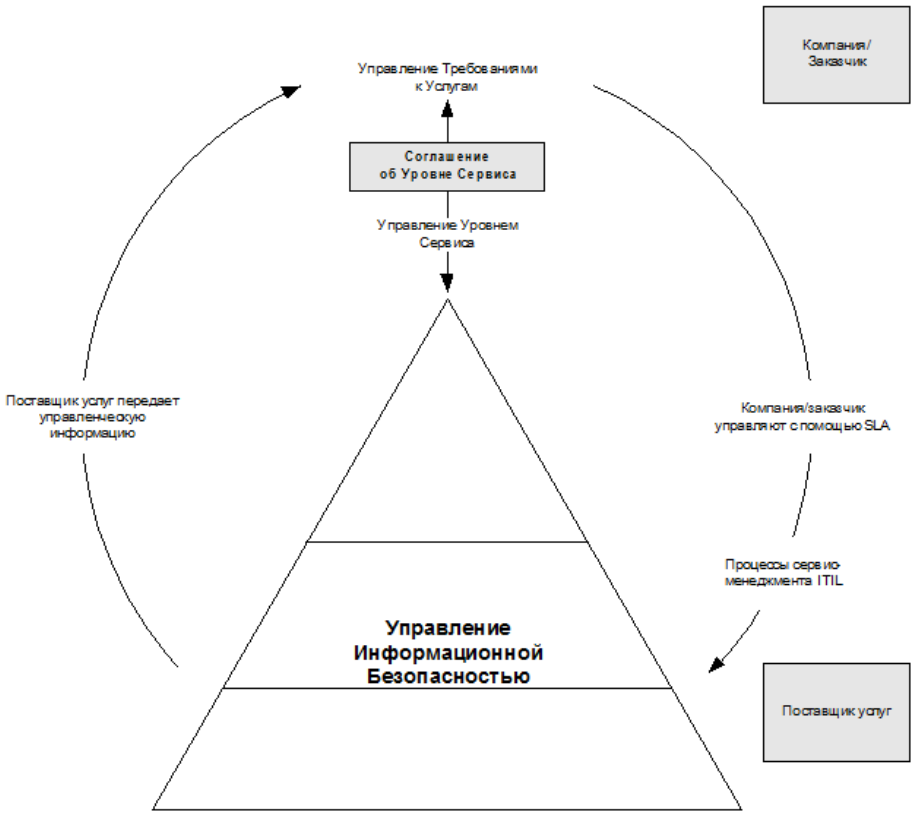


Рисунок 2.3. Отношения между процессами (источник: OGC)

Эти бизнес-процессы зависят от ИТ-услуг; а поэтому и от ИТ-организации. Заказчик определяет требования к безопасности (требования к информационной безопасности SLA на рис. 3. отсутствуют) на основе анализа риска. На рисунок 2.4. показано, как определяются элементы безопасности SLA.

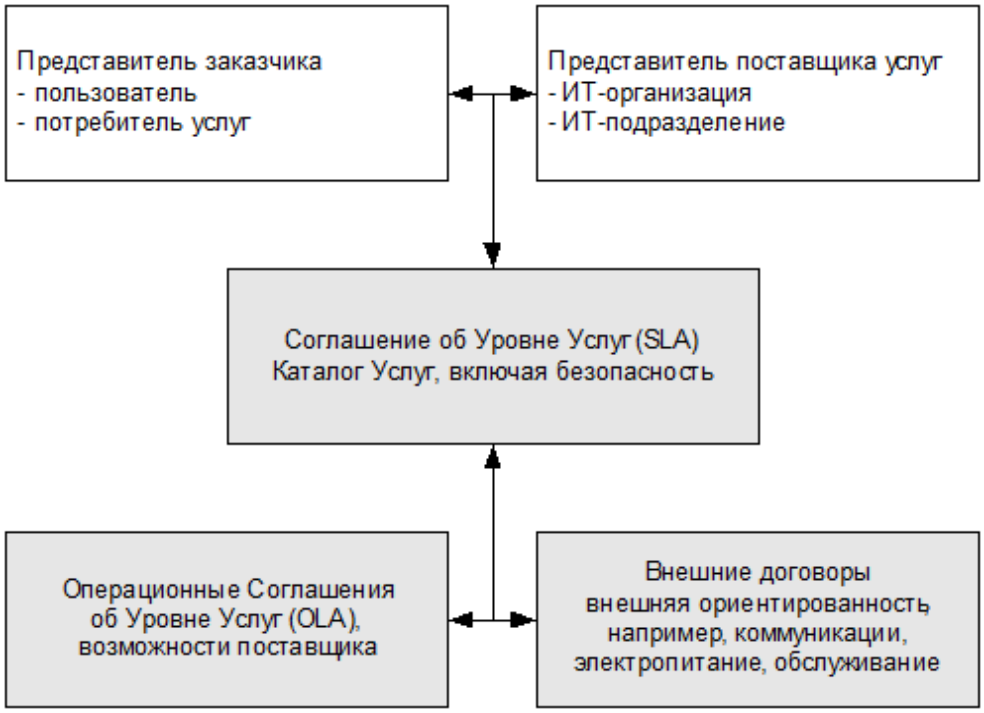


Рис. 2.4. Составление раздела по безопасности в соглашении SLA (источник: OGC)

Элементы безопасности обсуждаются представителями заказчика и поставщика услуг. Поставщик услуг сравнивает требования к Уровню Услуг Заказчика со своим Каталогом Услуг, где описываются стандартные меры безопасности (базовый Уровень Безопасности). Заказчик может выдвигать дополнительные требования.

Заказчик и поставщик сравнивают требования по Уровню Услуг с Каталогом Услуг. В разделе соглашения SLA по безопасности могут рассматриваться такие вопросы, как общая политика информационной безопасности, список авторизованного персонала, процедуры защиты ресурсов, ограничения на копирование данных и т. д.

2.3 Раздел по Безопасности Операционного Соглашения об Уровне Услуг (OLA)

Еще одним важным документом является Операционное Соглашение об Уровне Услуг. В нем описываются услуги, предоставляемые внутренним поставщиком услуг. Поставщик должен связать эти договоренности с видами ответственности, существующими внутри организации. В Каталоге Услуг дается их общее описание. В Операционном Соглашении об Уровне Услуг эти общие описания преобразуются в конкретные определения всех услуг и их компонентов, а также способа выполнения договоренностей об Уровнях Услуг внутри организации.

Пример. В Каталоге Услуг значится "управление авторизацией пользователей и частных лиц". Операционное Соглашение об Уровне Услуг конкретизирует это для всех определенных услуг, предоставляемых ИТ-организацией. Таким образом, реализация мероприятия определяется для подразделений, предоставляющих услуги UNIX, NT, Oracle и т. д.

Там, где это возможно, требования заказчика к Уровню Сервиса определяются по Каталогу Услуг, а в случае необходимости заключаются дополнительные соглашения. Такие дополнительные меры повышают Уровень Безопасности по сравнению со стандартным.

При составлении соглашения SLA необходимо согласовывать с Управлением Информационной Безопасностью измеряемые Ключевые показатели эффективности (KPI) и критерии. Показатели эффективности должны быть измеряемыми параметрами (метриками), а критерии эффективности должны устанавливаться на достижимом уровне. В некоторых случаях бывает трудно достичь договоренности по измеряемым параметрам безопасности. Их легче определить для доступности сервиса, которая может иметь цифровое выражение. Однако для целостности и конфиденциальности сделать это значительно труднее. Поэтому в разделе по безопасности в соглашении SLA необходимые меры обычно описываются

абстрактным языком. Практические нормы по Управлению Информационной Безопасностью используются как базовый комплекс мер безопасности. В соглашении SLA также описывается метод определения эффективности. ИТ-организация (поставщик услуг) должна регулярно предоставлять отчеты организации пользователя (заказчика).

2.4 Построение комплексной системы информационной безопасности организации

Любая организация, вне зависимости от размера и типа, подвержена действию разрушающих инцидентов. Эти инциденты могут носить как чрезвычайный (например, природные катаклизмы, эпидемии), так и, что более вероятно, бытовой характер (прорыв трубопровода, отключение электроэнергии и т. п.). Вызванные ими нарушения в работе организации влияют на потребителей и другие заинтересованные стороны, вызывая финансовые потери и негативно влияя на репутацию организации. Менеджмент непрерывности бизнеса является мощным инструментом, помогающим организациям управлять рисками возникновения инцидентов всех типов. Для большинства организаций менеджмент непрерывности бизнеса включает процессы восстановления функционирования в случае чрезвычайных ситуаций, кризис-менеджмента и др.

Система менеджмента непрерывности бизнеса позволяет уменьшить вероятность возникновения разрушающего инцидента и повышает готовность организации быстро и должным образом реагировать на его возникновение и тем самым уменьшить потенциальный ущерб.

В стандарте ISO 22301 устанавливаются требования к внедрению, функционированию и улучшению системы непрерывности бизнеса. Кроме того, в нем требуется идентифицировать критические факторы риска, воздействующие на организацию, понимать потребности и обязательства организации, измерять способность организации справляться с

разрушающими инцидентами, гарантировать соответствие заявленной политике в области непрерывности бизнеса и др. Стандарт предназначен для целей сертификации, что позволяет продемонстрировать потребителям и партнерам надежность организации. Требования стандарта носят универсальный характер и могут быть применены любой организацией, вне зависимости от типа, размера или вида деятельности.

Современные организации обладают, как правило, сложной, территориально распределенной корпоративной информационной системой и большим количеством критичных информационных ресурсов и работают в условиях растущих репутационных рисков и непрерывно меняющихся внешних требований к защите информации.

В такой ситуации обеспечить безопасность и защиту информации в информационных системах при адекватных расходах возможно лишь при использовании системного подхода, который подразумевает последовательное внедрение в компании комплексной системы информационной защиты и безопасности (КСИБ).

Наличие КСИБ позволяет снизить правовые, финансовые, репутационные и операционные риски, связанные с безопасностью информации, обеспечить соответствие всем актуальным для организации требованиям, оптимизировать организационную структуру и финансовые расходы на обеспечение информационной безопасности.

КСИБ включает в себя набор взаимосвязанных организационных мер, программно-технических средств и процессов управления на всех уровнях деятельности организации: стратегическом, тактическом и операционном.

Полную систему услуг и решений, необходимых для построения КСИБ. В рамках системы КСИБ можно выделить группы услуг по различным направлениям обеспечения ИБ организации:

- услуги по управлению ИБ (ГУС-1);
- услуги по обеспечению ИБ (ГУС-2);
- услуги по обеспечению соответствия требованиям (ГУС-3);

- услуги по сопровождению систем и процессов ИБ (ГУС-4);
- услуги по аттестации и лицензионной работе (ГУС-5);
- услуги по подготовке и повышению квалификации кадров для работы в комплексной системе информационной безопасности организации (ГУС-6);
- услуги по расследованию компьютерных преступлений (ГУС-7).

Услуги и решения по управлению ИБ направлены на построение в организации эффективных процессов управления, которые обеспечивают:

- предоставление максимально полной и достоверной информации о состоянии информационной безопасности на всех уровнях управления организацией;
- эффективный обмен информацией между всеми заинтересованными сторонами: руководством организации, акционерами, клиентами и партнерами, регулирующими органами и органами по сертификации;
- принятие правильных и своевременных решений на всех уровнях управления организацией в условиях внешних и внутренних изменений;
- оптимизацию финансовых расходов на информационную безопасность.

Услуги и решения по обеспечению ИБ направлены на защиту информации и информационной системы организации от внешних и внутренних угроз информационной безопасности, в том числе:

- угроз несанкционированного доступа и несанкционированного использования информационных ресурсов;
- угроз утечки и разглашения конфиденциальной информации;
- угроз, возникающих при взаимодействии с сетью, безопасностью в Интернете и другими внешними сетями;
- угроз нарушения целостности или доступности информационных ресурсов;

- других угроз информационной безопасности.

Услуги и решения по обеспечению соответствия требованиям направлены на защиту информации в соответствии с актуальными требованиями законодательства РФ, контролирующих, регулирующих и сертификационных органов, в том числе:

- с Законом № 152 ФЗ «О персональных данных»;
- стандартом международных платежных систем PCI DSS;
- стандартом Банка России СТО БР ИББС;
- международным стандартом ISO IEC 27001:2005;
- другими требованиями в области информационной безопасности.

Услуги по сопровождению систем и процессов ИБ

Для обеспечения максимальной надежности и доступности внедренного решений обеспечения ИБ организации может использоваться услуга по расширенной технической поддержке, которая включает в себя поддержку по телефону или оперативные выезды для решения возникших локальных проблем ИБ.

Услуга по сопровождению внедренного решения может также включать в себя консультационную поддержку и инспекционные визиты для оценки эффективности функционирования внедренных процедур и программно-технических средств и устранения выявленных проблем.

Например, для поддержания Системы защиты персональных данных в актуальном состоянии требуется ее регулярная доработка. Обусловлено это следующими факторами:

- меняется состав персональных данных, обрабатываемых в ИСПДн компании.
- меняется состав ИСПДн
- проходит реструктуризация подразделений
- возможно изменение законодательства в области персональных данных

и т.д.

С целью решения данной задачи должны быть предложена комплексная услуга «Сопровождение системы защиты персональных данных, разработанной », в состав которой входит:

Услуги по подготовке и повышению квалификации кадров для работы в комплексной системе информационной безопасности организации включают организацию взаимодействия сотрудников коллектива организации и обучение специалистов Заказчика, т.к. наличие квалифицированных специалистов является ключевым фактором для успешного внедрения и последующего эффективного функционирования внедряемых процессов и систем.

Услуги по расследованию компьютерных преступлений

Ежедневно инциденты, связанные с информационной безопасностью, происходят в организациях по всему миру. Не существует 100%-ной защиты, всегда остаются риски, которые могут быть реализованы случайно или намеренно. Профиль рисков для каждой организации уникален. При этом многие риски не рассматриваются совсем либо механизмы их снижения не соответствуют их уровню. Это потенциально ставит организацию перед возможными негативными событиями, такими как кража ценной информации, утечка персональных данных, нарушение работоспособности интернет-ресурсов, причинение предприятию ущерба репутации и др.

В основном инциденты, представляющие риск для организации и требующие немедленного реагирования, можно разделить на внутренние (например, утечка конфиденциальных данных, аномальная сетевая активность, компрометация информации и т.д.) и внешние (например, DDoS-атаки, фишинг, попытки взлома и сканирования портала и т.д.). Перечень инцидентов чрезвычайно широк.

Услуга по оперативному реагированию на инциденты включает:

- немедленную консультацию сертифицированных специалистов;

- оперативную разработку и помощь в реализации плана реагирования на инцидент с учетом мировых практик управления инцидентами ИБ и особенностей организации заказчика;
- оперативное устранение критичных уязвимостей;
- разработку рекомендаций по улучшению мер защиты информации;
- разработку плана и набор рекомендаций по расследованию инцидента;
- оперативное предоставление информации по первоначальным этапам расследования и рекомендаций по оперативному восстановлению бизнес-процессов;
- предоставление полного списка необходимых действий для полного восстановления после инцидента;
- предоставление полного отчета, включающего информацию о проделанной работе;
- собрание участвующих в совместной работе лиц для обсуждения проделанной работы по устранению инцидента и прояснения всех деталей.

В кратчайшие сроки предоставляется максимально полная информация о произошедшем инциденте и путях его локализации независимо от того, была ли это атака на сайт, систему банковского обслуживания, программное обеспечение или любые другие информационные активы.

В процессе реагирования разрабатывается оперативный план действий, нацеленный на скорейшее сдерживание инцидента, снижение ущерба и восстановление критичных бизнес-процессов.

На сегодня разработчики ИБ- и ИТ-решений предлагают системы управления инцидентами. Однако одних только технических средств недостаточно. «Интеллектуальные» инциденты со стороны злоумышленников, учитывающие контур защиты заказчика, прошлый опыт неправомерного доступа к его информационным активам, могут быть

предотвращены только «двойным» инструментарием – оборудованием и опытным экспертом, умеющим грамотно его настроить и квалифицированно применить.

Услуги по аттестации и лицензионной работе

Реализация данной услуги кроме повышения общего уровня защищенности эксплуатируемых информационных ресурсов позволяет организации:

- получить официальное подтверждение эффективности и достаточности принятых на объекте информатизации мер защиты, а также их соответствия требованиям действующих нормативно-методических документов;
- получить официальное подтверждение готовности объекта информатизации к обработке конфиденциальной информации (информации, составляющей государственную тайну);
- подготовить организацию – соискателя лицензии к получению лицензий ФСТЭК России на осуществление работ, связанных с деятельностью по технической защите конфиденциальной информации, и ФСБ России на осуществление работ, связанных с использованием шифровальных (криптографических) средств;
- повысить доверие к организации со стороны государственных органов, ведомств, клиентов, взаимодействующих организаций и партнеров.

Детализируем представленные выше услуги.

Услуги в области управления ИБ

- Разработка стратегии информационной безопасности
- Аудит Информационной безопасности
- Построение Системы управления ИБ (СУИБ) в соответствии с ISO 27001
- Построение системы внутреннего аудита и обеспечения соответствия требованиям политик ИБ
- Построение системы управления информационными рисками

- Построение системы обеспечения непрерывности бизнес-процессов (BS25999)
- Услуги по мониторингу информационной безопасности 24/7 (MSS)

Услуги по обеспечению информационной безопасности

- Защита банкоматов и критичных систем
- Построение системы противодействия утечке конфиденциальной информации (DLP)
- Построение системы контроля устройств ввода–вывода информации
- Построение корпоративной системы контроля входящего веб-трафика (WEB-фильтрация)
- Построение корпоративной системы шифрования данных
- Построение корпоративной системы идентификации и аутентификации
- Построение корпоративной инфраструктуры открытых ключей - PKI (Корпоративный Удостоверяющий центр - УЦ)
- Построение системы антивирусной защиты серверов и рабочих станций
- Построение корпоративной системы защиты каналов связи (VPN)
- Построение системы обнаружения и предотвращения атак и вторжений (IPS, IDS)
- Построение корпоративной системы межсетевого экранирования (firewall)
- Построение системы удаленного защищенного доступа
- Построение системы резервного копирования и восстановления данных
- Построение системы архивирования корпоративной почты
- Обеспечение защиты мобильных устройств

- Построение системы сбора, корреляции событий и управления инцидентами информационной безопасности
- Построение системы управления уязвимостями
- Обеспечение безопасности сетевой инфраструктуры
- Построение корпоративной системы защиты беспроводных сетей

Услуги в области соответствия требованиям

- Защита персональных данных
- Приведение инфраструктуры компании в соответствие требованиям стандарта PCI DSS
- Управление уязвимостями в соответствии с требованиями PCI DSS
- Обеспечение соответствия требованиям СТО БР ИББС
- Услуги по защите информационных ресурсов, собственником которых является государство (государственная тайна, конфиденциальная информация)
- Защита информации в национальной платежной системе

Услуги по аттестации и лицензионной работе

- Подготовка организаций к получению лицензий ФСТЭК и ФСБ России
- Аттестация информационных систем на соответствие требованиям государственных и отраслевых регуляторов по информационной безопасности

Услуги по расследованию компьютерных преступлений

- Реагирование на инциденты ИБ
- Расследование инцидентов ИБ
- Программы сопровождения и поддержки
- Юридическое сопровождение дел по расследованию инцидентов
- Защита от DDoS-атак
- Антифрод (предотвращение мошенничества в системах ДБО)

- Услуги лаборатории компьютерной криминалистики
- Восстановление данных
- Безопасный бренд

Услуги по сопровождению систем и процессов ИБ

- Техническая консультация - Письменный (по электронной почте) или устный (по телефону) ответ на стандартные вопросы по установке, настройке, функционированию или особенностям работы программного обеспечения.
- Предоставление новых версий программных продуктов на материальном носителе или предоставлением ссылки в сети Интернет для получения и установки данных обновлений.
- Плановый профилактический выезд технических специалистов для проведения профилактических работ по диагностированию параметров работы Системы и исправлению существующих проблем.
- Аварийный выезд специалиста - аварийный выезд на объект для проведения восстановительных работ.
- Выезд на место инцидента в случае проведения контрольных мероприятий Уполномоченными органами, с целью представления его интересов
- Аналитические и/или юридические консультации
- Профессиональные консультации специалистов по защите ПДн
- Внесение изменений/корректировка существующей документации по защите ПДн, а также разработка дополнительной документации, адаптация документов по защите ПДн к новым (изменённым) бизнес- процессам клиента
- Внесение изменений в настройку средств защиты ПДн, установка новых или дополнительных модулей
- Дополнительная Техническая поддержка – любые дополнительные услуги по сопровождению внедренных систем.

Услуги по подготовке и повышению квалификации кадров для работы в комплексной системе информационной безопасности

- Подготовка и обновление методических рекомендаций для различных категорий работников организации по обеспечению ее ИБ.
- Тестирование на знание нормативно-правовой базы обеспечения ИБ на соответствующем уровне ответственности работника организации.
- Подготовка и переподготовка сотрудников предприятия на основе системы модулей компетенций в области ИБ.
- Контроль знаний сотрудников организации с выдачей соответствующего уровню обеспечения ИБ сертификата.

Глава 3. Оценка риска ИБ

На основе стандарта ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности: Менеджмент риска информационной безопасности» (ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management (IDT)) рассмотрим процесс управления риском информационной безопасности получения образования в системе дистанционного обучения. Опишем типовые поды оценки риска организации на примере системы дистанционного обучения.

Процесс управления риском информационной безопасности

Процесс менеджмента риска ИБ состоит из 1) установления контекста; 2) оценки риска; обработки риска; 3) принятия риска; 4) коммуникаций риска; 5) мониторинга и переоценки риска ИБ (Рисунок 3.1).

Конец первой или последующих итераций

Рисунок 3.1. - Процесс менеджмента риска информационной безопасности

Процедуры оценки риска и обработки риска в процессе менеджмента риска ИБ могут выполняться итеративно, такой подход к проведению оценки риска может увеличить детализацию и глубину оценки при каждой последующей итерации. Если для эффективного определения действий удается получить достаточную информацию на очередном шаге итерации, необходимую для снижения риска до требуемого уровня, то считается, что задача этапа выполнена, затем идет этап обработки риска. В случае недостаточности информации для принятия решения, пересматривается контекст и осуществляется очередная итерация оценки риска (критериев оценки, влияния или принятия рисков), возможно для некоторой отдельной части полной предметной области, которая ограниченна первой точкой принятия решения.

Эффективность обработки риска непосредственно зависит от результатов получаемых при оценке риска. Первоначальная обработка риска может не обеспечить необходимый уровень остаточного риска. В этом случае могут потребоваться, дополнительные итерации оценки риска с изменением соответствующих параметров контекста (критериев оценки, влияния и принятия риска), за каждой из которых последует соответствующая шагу итерации процедура обработки риска, запускаемая на второй точке принятия решения (рисунок 3.1).

Установление контекста, оценка, разработка плана обработки, принятие риска в системе менеджмента информационной безопасности (СМИБ) представляют собой раздел фазы «планирование». В фазе «осуществление» СМИБ по плану обработки риска реализуются процедуры и меры для снижения риска до требуемого уровня. Руководство в фазе «проверка» СМИБ устанавливает необходимость оценки и обработки риска повторно из за появившихся инцидентов и изменившихся обстоятельств. Проведение необходимых работ, по поддержке и усовершенствованию процесса менеджмента риска ИБ происходит в фазе «действие». В таблице

3.1 показаны четыре фазы процесса СМИБ во взаимосвязи с процедурами менеджмента риска.

Таблица 3.1

Соотношение процесса менеджмента риска информационной безопасности и компонентов процесса системы менеджмента информационной безопасности

Процесс СМИБ	**Процесс менеджмента риска ИБ**
Планирование	Установление контекста
	Оценка риска
	Планирование обработки риска
	Принятие риска
Осуществление	Реализация плана обработки риска
Проверка	Проведение непрерывного мониторинга и переоценки рисков
Действие	Поддержка и усовершенствование процесса менеджмента риска ИБ

В процессе менеджмента риска информационной безопасности выделим и детализируем процесс оценки риска ИБ и изобразим его в виде схемы на рисунке 3.2.

Рисунок 3.2. Детализированный процесс оценки риска ИБ

USED AT:	AUTHOR: Бочаров М.И.	DATE: 09.06.2014	WORKING	READER	DATE	CONTEXT:
	PROJECT: Процесс менеджмента риска ИБ	REV: 09.06.2014	DRAFT			TOP
			RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		PUBLICATION			

NODE:	TITLE:	NUMBER:
1	Процесс менеджмента риска ИБ дистанционной образовательной услуги	1

3.1 Установление контекста

Входные данные. Вся информация об оказании дистанционных образовательных услуг организации, имеющая отношение к контексту менеджмента риска ИБ.

Анализ организации

Основная цель организации. Дистанционное оказание услуг получения образования

Структура организации:

- Администрация.
- Кафедры.
- Организационно-методический отдел.
- Отдел маркетинга.
- IT-отдел.
- Бухгалтерия.

Стратегия организации. Оказание качественных образовательных услуг с использованием современных способов представления электронного образовательного контента, средств удаленного доступа к образовательному контенту.

Действие. Задача данного этапа заключается в установлении контекста менеджмента риска ИБ, в эту процедуру входит определение основных критериев, необходимых для менеджмента риска ИБ, а также установление области применения и границ и создание соответствующей организационной структуры, обеспечивающей менеджмент риска ИБ.

Функциональные ограничения. Круглосуточная работа сервиса, для непрерывно обеспечения доступа к образовательным ресурсам.

Ограничения, касающиеся персонала. Наличие специалиста по ИБ.

Ограничения культурного свойства. Образование, обучение, профессиональный опыт, работу, на которую распространяется жизненный опыт, мнения, философию, убеждения, чувства, социальный статус и т.д.

Нормативные требования, относящиеся к деятельности образовательной организации. К их числу могут быть отнесены законы, постановления, специальные инструкции, относящиеся к сфере деятельности организации или внутренним/внешним нормам. Это касается также договоров и соглашений и любых обязательств юридического свойства.

Технические ограничения.

Относящиеся к инфраструктуре технические ограничения, как правило, возникают от функционирующих в образовательной организации аппаратных и программных средств и от площадок или помещений, где осуществляются процессы:

- Файловые архивы - требования, относительно организации, менеджмент носителей, менеджмент правил доступа и т.д.;
- общая архитектура - требования, относительно топологии (централизованная архитектура, распределенная архитектура, архитектура клиент-сервер, физическая архитектура и т.д.);
- прикладные программы для организации дистанционного обучения - требования, относительно проектирования специфичного программного обеспечения удовлетворяющего особые потребности системы дистанционного обучения, рыночные стандарты и т.д.;
- аппаратные средства - требования, относящиеся к стандартам, качества, соответствию нормам и т.д.;
- сети связи - требования, относящиеся к стандартам организации сетей, расширяемости, масштабируемости, надежности и т.д.;

Ограничения по времени. Если на реализацию мер и средств контроля и управления безопасностью уходит слишком много времени, то риски, для которых разрабатывалась система мер и средств контроля и управления,

могут измениться. При принятии решений и выборе приоритетов время является определяющим фактором.

Организационные ограничения. Требований организации накладывают определенные ограничения:

- эксплуатация - требования, касающиеся предоставления услуг, длительности производственного цикла, мониторинга, наблюдения, ухудшения работы, планов действий в чрезвычайных ситуациях и др.;
- поддержка - требования к процедуре поиска неисправностей, связанных с инцидентом, осуществлению превентивных действий, быстрому исправлению и др.;
- менеджмент кадровых ресурсов - требования, относящиеся к обучению операторов и пользователей, до уровня квалификации, необходимой для таких должностей, это могу быть должности системного администратора или администратора данных и др.;
- административный менеджмент – требования к персоналу, касающиеся обязанностей и др.;
- менеджмент разработки - требования, относящиеся к инструментальным средствам разработки, требования к системе автоматизированной разработки программ, планов приемочного контроля и др.;
- менеджмент внешних отношений - требования, относящиеся к формированию отношений с третьими сторонами, договоров и т.д.

Руководство по реализации. Цель менеджмента риска ИБ в дистанционном образовании:

- поддержка СМИБ;
- подготовка плана обеспечения непрерывности бизнеса по осуществлению дистанционной образовательной услуги;
- подготовка плана реагирования на инциденты;
- описание требований ИБ для образовательной услуги.

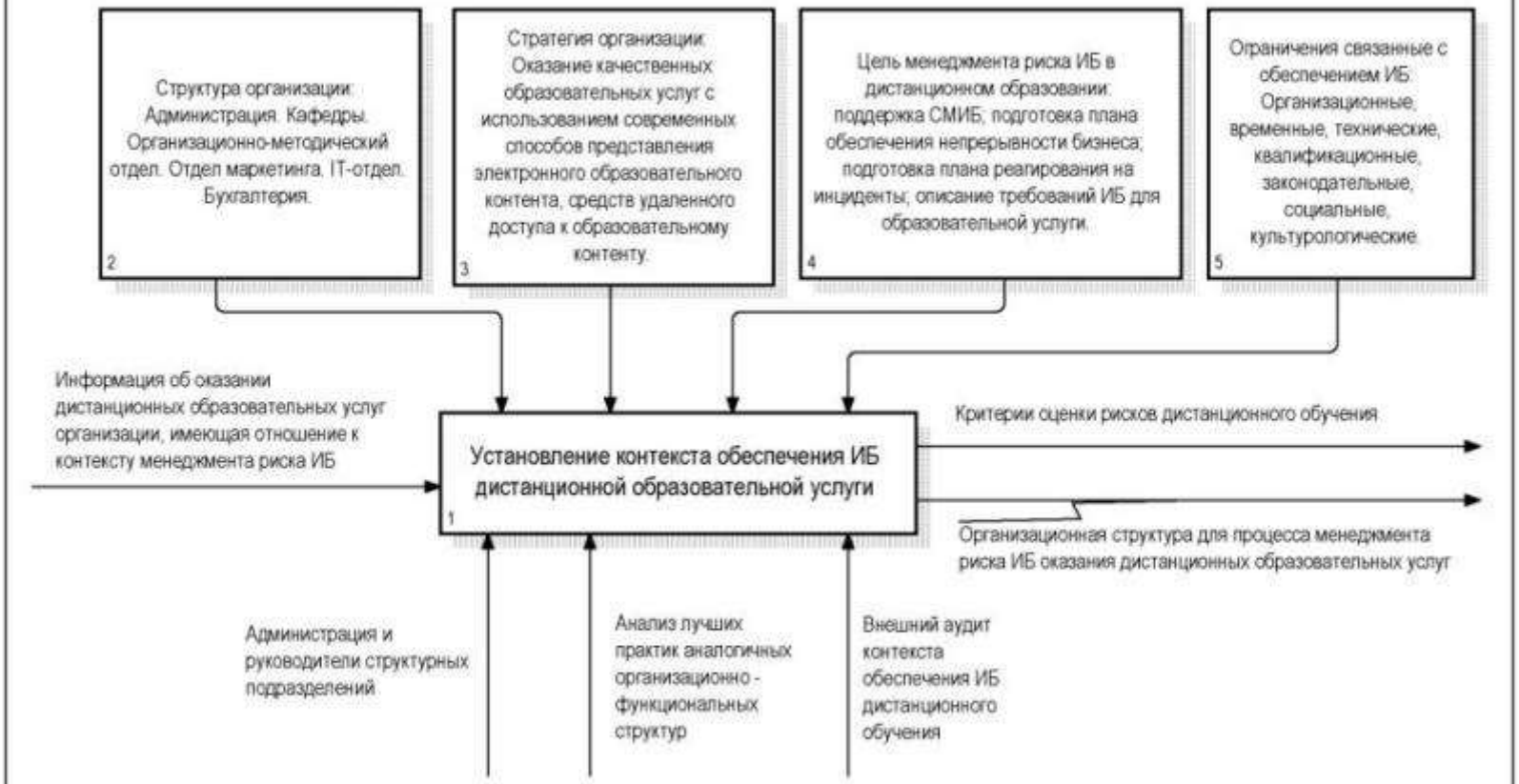
Выходные данные. Спецификация основных критериев, границы, сфера действия, организационная структура для процесса менеджмента риска ИБ.

Критерии оценки рисков информационной безопасности

Критерии для оценки рисков информационной безопасности образовательной организации выбираются с учетом:

- стратегической ценности обработки бизнес-информации (интеллектуальный труд преподавателей разработчиков электронных курсов);
- критичности затронутых информационных активов (персональные данные студентов);
- законодательно-нормативных требований и договорных обязательств (предоставление образовательных услуг соответствующего уровня объема и качества);
- оперативного значения и значения для бизнеса доступности, конфиденциальности и целостности (доступности курсов студентам и доступа к личному кабинету для управления предметной образовательной средой в рамках своих курсов, конфиденциальности доступа и целостности образовательного контента);
- ожидания и реакции причастных сторон, а также негативных последствий для нематериальных активов и репутации образовательного учреждения.

USED AT:	AUTHOR: Бочаров М.И.	DATE: 09.06.2014	■	WORKING	READER	DATE	CONTEXT:
	PROJECT: Установление контекста обеспечения ИБ дистанционной образовательной услуги	REV: 09.06.2014		DRAFT			TOP
	NOTES: 1 2 3 4 5 6 7 8 9 10			RECOMMENDED			
				PUBLICATION			



NODE:	TITLE:	NUMBER:
1	Установление контекста обеспечения ИБ дистанционной образовательной услуги	2

3.2 Оценка риска информационной безопасности

Общее описание оценки риска информационной безопасности

Входные данные. Установленные основные критерии, сфера действия и границы, структура процесса менеджмента риска информационной безопасности, принятые для организации оказывающей дистанционные образовательные услуги.

Действие. Необходимо идентифицировать риски, количественно или качественно их охарактеризовать, назначить для них приоритеты в соответствии с критериями оценки риска и целями образовательной организации.

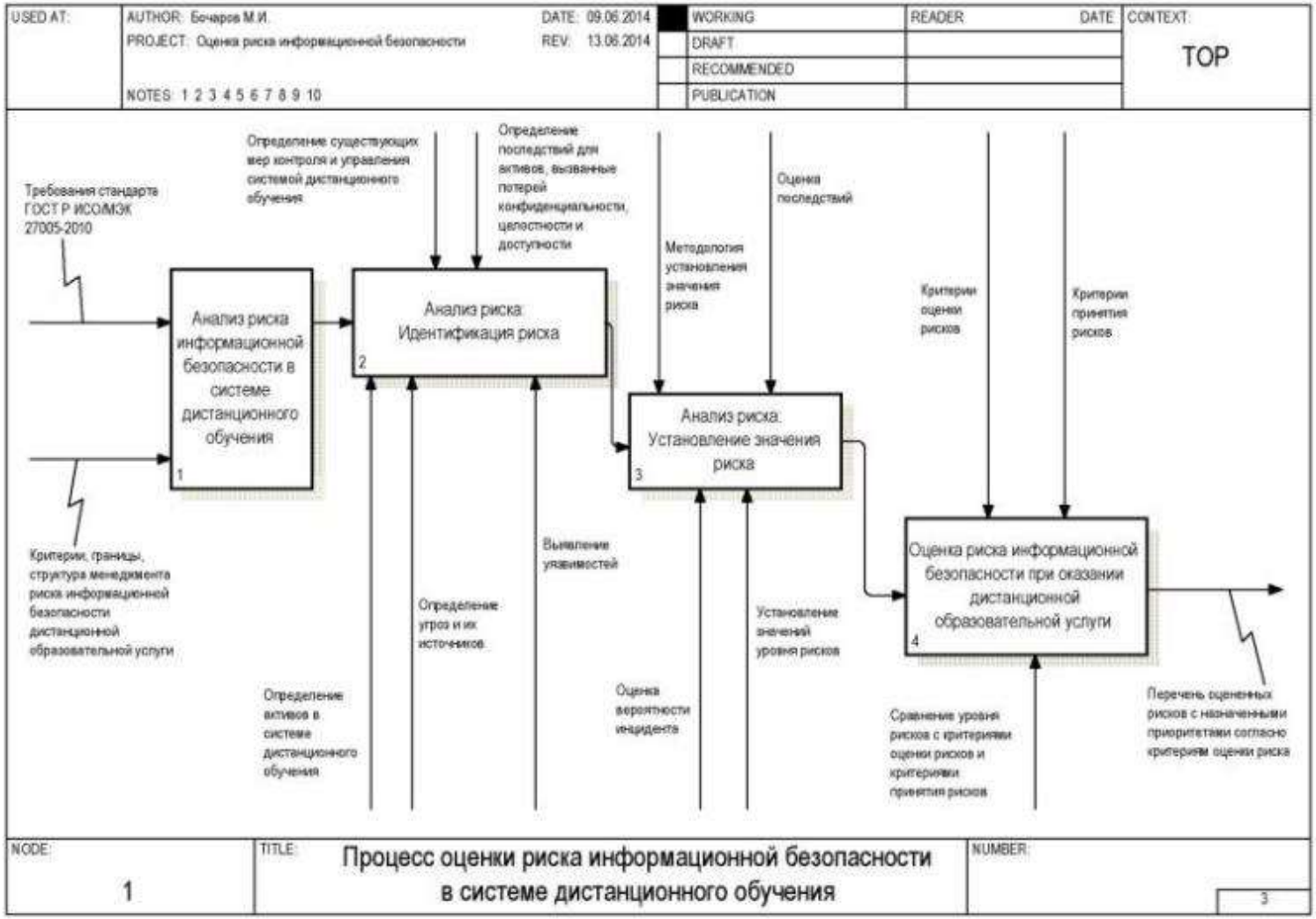
Руководство по реализации. Риск представляет собой комбинацию последствий, вытекающих из нежелательного события и вероятности возникновения события.

Оценка риска количественно или качественно характеризует риски и дает руководителям возможность назначать для рисков приоритеты в соответствии с осознаваемой руководством серьезностью или другими установленными критериями.

Процесс оценки риска состоит из:

- анализа риска, включающего идентификацию риска и установление значения риска;
- оценки риска .

Выходные данные. Перечень оцененных рисков в соответствии с назначенными приоритетами согласующимся с критериями оценки риска.


USED AT:
AUTHOR: Бочаров М.И.
DATE: 09.06.2014
PROJECT: Оценка риска информационной безопасности
REV: 13.06.2014
NOTES: 1 2 3 4 5 6 7 8 9 10
WORKING
DRAFT
RECOMMENDED
PUBLICATION
READER
DATE
CONTEXT:
TOP
Требования стандарта ГОСТ Р ИСО/МЭК 27005-2010
Определение существующих мер контроля и управления системой дистанционного обучения
Определение последствий для активов, вызванные потерей конфиденциальности, целостности и доступности
Методология установления значения риска
Оценка последствий
Критерии оценки рисков
Критерии принятия рисков
Анализ риска информационной безопасности в системе дистанционного обучения
1
Анализ риска: Идентификация риска
2
Анализ риска: Установление значения риска
3
Оценка риска информационной безопасности при оказании дистанционной образовательной услуги
4
Критерии, границы, структура менеджмента риска информационной безопасности дистанционной образовательной услуги
Определение активов в системе дистанционного обучения
Определение угроз и их источников
Выявление уязвимостей
Оценка вероятности инцидента
Установление значений уровня рисков
Сравнение уровня рисков с критериями оценки рисков и критериями принятия рисков
Перечень оцененных рисков с назначенными приоритетами согласно критериям оценки риска
NODE:
1
TITLE:
Процесс оценки риска информационной безопасности в системе дистанционного обучения
NUMBER:
3

3.3 Анализ риска: идентификация риска

Цель идентификации риска - в определении того, что может произойти при нанесении возможного ущерба, и в получении представлений о том, как, где и почему мог иметь место такой ущерб. Следующие ниже этапы, должны объединять входные данные для деятельности по количественной оценке риска.

3.3.1 Определение активов

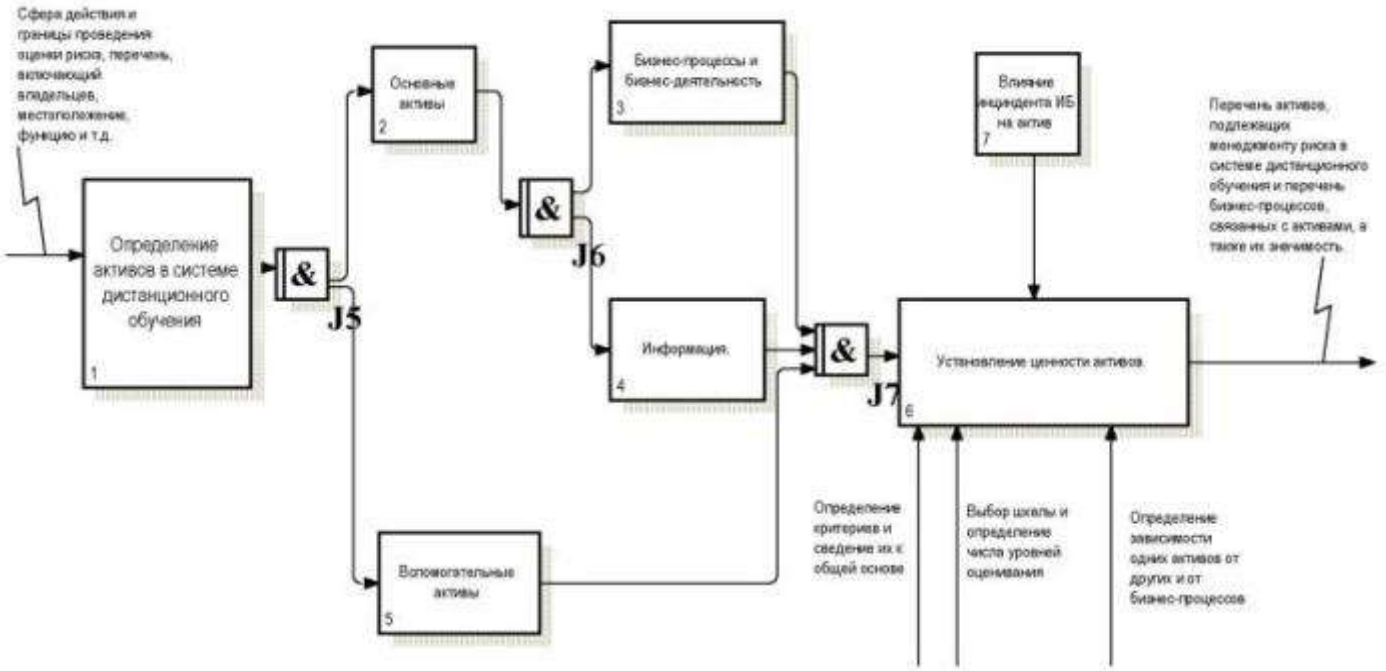
Входные данные. Сфера действия и границы этапа проведения оценки риска, перечень, включающий местоположение, владельцев, функцию и т.д.

Действие. Определяем активы, входящие в установленную сферу действия.

Руководство по реализации. Активом является что-либо, имеющее ценность для организации и, поэтому, нуждающееся в защите. При определении активов необходимо учитывать, что информационная система состоит не только из программных и аппаратных средств.

Выходные данные. Перечень активов, подлежащих менеджменту риска, а также перечень бизнес-процессов, связанных с активами и их значимость.

USED AT:	AUTHOR: Бечаров М.И.	DATE: 09.06.2014	WORKING	READER	DATE	CONTEXT:
	PROJECT: Оценка риска информационной безопасности	REV: 14.06.2014	DRAFT			TOP
			RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		PUBLICATION			



NODE:	TITLE:	NUMBER:
1	Определение активов в системе дистанционного обучения	4

Определение и установление ценности активов и оценка влияния

Чтобы установить ценность активов, организация должна, в первую очередь, определить все принадлежащие ей активы на соответствующем уровне детализации. Различают два вида активов:

- основные активы, содержащие бизнес-процессы, бизнес-деятельность и информацию;
- вспомогательные (поддерживающие) активы, от них зависят основные составные части области применения всех типов, содержащие программное обеспечение, аппаратные средства, сеть, место функционирования организации, персонал, структуру организации.

Основными активами как правило являются базовые процессы и информация о деятельности организации дистанционно оказывающей образовательные услуги в ее сфере действия. Также могут рассматриваться и другие основные активы, такие, как процессы жизнедеятельности организации, которые будут иметь отношение к формированию политики ИБ или плана непрерывности бизнеса. В зависимости от цели, не всегда требуется исчерпывающий анализ всех элементов, составляющих процесс менеджмента риска. В таких случаях область изучения может быть ограничена наиболее значимыми элементами.

Основные активы бывают двух типов:

1. Бизнес-процессы (или подпроцессы) и бизнес-деятельность, например:

- процессы, утрата и/или ухудшение которых делает невозможным реализацию целей и задач организации;
- процессы, содержащие засекреченные процессы и/или процессы, созданные с использованием патентованной технологии;
- процессы, модификация которых может значительно повлиять на реализацию основных целей и задач организации;

- процессы, необходимые организации для выполнения договорных, нормативных или законодательных требований.

2. Информация. Основная информация, по большей части, включает в себя:

- информацию, которая необходима для реализации назначения или бизнеса организации;
- информацию личного характера, которая в соответствии с национальным законам о неприкосновенности частной жизни определена особым образом;
- стратегическую информацию, которая необходима для достижения целей, определяемых направлением стратегии организации;
- ценную информацию, обработка и передача, сбор и хранение которой требуют продолжительного времени или связаны с большими затратами на ее приобретение.

Основные активы в системе дистанционного обучения:

- Процесс поступления-приема на дистанционную форму обучения.
- Процесс формирования образовательного контента.
- Процесс получения обучающимся образовательных материалов.
- Процесс дистанционного оказания обучающемуся консультационных услуг.
- Процесс отчетности обучающегося и оценка работы обучающегося.
- Процесс перевода обучающегося на следующий образовательный этап.
- Процессы маркетинга и обслуживания сайта образовательной организации и системы дистанционного обучения.
- Информация о персональных данных учащихся и персонала системы дистанционного обучения.

- Информация о финансовом состоянии организации, предоставляющей услугу дистанционного получения образования.
- Информационные ресурсы базы данных образовательных электронных курсов

Вспомогательным активам присущи уязвимости, которыми могут воспользоваться угрозы, нацеленные на порчу основных активов области рассмотрения (процессов и информации). Активы могут быть различных типов.

Аппаратные средства:

Серверы, персональные электронные устройства с доступом в сеть Интернет.

Программные средства:

Операционная система.

Антивирусные средства.

Программная среда для организации дистанционного обучения на основе Moodle. Браузеры и плагины к ним для доступа к среде дистанционного обучения.

Сеть:

Телекоммуникационные устройства, используемые для соединения нескольких физически удаленных компьютеров или элементов информационной системы.

Устройства, являющиеся не оконечными, а промежуточными устройствами связи. Ретрансляторы, мосты, маршрутизаторы, коммутаторы, концентраторы.

Сетевое программное обеспечение управления и мониторинга активного сетевого оборудования. Генерация журналов регистрации.

Персонал:

Администрация организации осуществляющей дистанционную образовательную деятельность.

Профессорско-преподавательский состав.

Менеджеры дистанционного образовательного процесса, специалисты учебной части, методисты, разработчики образовательного контента и контента сайта образовательной организации.

Руководитель отдела кадров, руководитель финансового отдела, руководитель, осуществляющий менеджмент риска.

Персонал по эксплуатации и сопровождению информационной системы.

Разработчики программных элементов среды дистанционного обучения и сайта образовательной организации.

Место функционирования организации:

Офис и серверная.

Внешний хостинг сайта.

Удаленные точки доступа к системе дистанционного обучения.

Организация:

Организация оказывающая образовательные услуги.

Структура организации:

Администрация. Кафедры.

Организационно-методический отдел.

Отдел маркетинга.

IT-отдел.

Бухгалтерия.

Установление ценности активов

Установление ценности активов заключается в согласовании используемой шкалы ценностей и критериев для присвоения каждому активу определенного положения на шкале, основанного на установлении ценности. Термины, обычно используемые для качественного установления ценности активов: критичная, очень высокая, высокая, средняя, низкая, очень низкая, пренебрежимо малая.

1) **Критерии**

Ценность некоторых активов, может, устанавливаться субъективно и принимать решения, возможно, будут разные люди. Вероятные критерии, используемые для определения ценности актива, включают его исходную стоимость, стоимость его замены или воссоздания, или ценность, которая может быть абстрактной, такая как ценность репутации организации.

Также основой для установления ценности активов являются расходы, которые могут быть понесены из-за потери конфиденциальности, целостности, учетности и доступности в результате инцидента. Неотказуемость, подлинность и надежность также должны рассматриваться определенным для этого образом.

2) Сведение к общей основе

Критерии, для установления ценности активов, сведенные к общей основе, могут использоваться при оценке возможных последствий, вытекающих из потери конфиденциальности, целостности, доступности, учетности, надежности, неотказуемости или подлинности активов, включают:

- **прерывание сервиса** - невозможность обеспечения доступа к системе дистанционного обучения;
- **утрата доверия клиента** - потеря репутации образовательной организации (распространение сведений характеризующих важность предоставляемых услуг для клиентов: выдача дипломов не соответствующих квалификации специалистов, низкое качество образовательных услуг, плохой сервис, необоснованное увеличение оплаты за обучение и др. сведения);
- **нарушение внутреннего функционирования** - нарушения внутри самой образовательной организации (которые могут возникнуть по причине ухода или болезни специалиста обслуживающего критические процессы, поиск специалиста соответствующей квалификации и требуемое время на адаптацию к условиям и используемым средствам дистанционного обучения повлекут дополнительные внутренние расходы);

- **нарушение функционирования третьей стороны** - нарушения в функционировании третьей стороны ведущей дела с образовательной организацией (это сбои в работе организации, предоставляющей хостинг для размещения сайта образовательной организации), что повлечет за собой различные виды убытков, как материальных в потере клиентов во время набора учащихся, так и репутационных, отражающихся на имидже образовательной организации;
- **нарушение законов/норм** - неспособность выполнения правовых обязательств; подразумевает несвоевременное получение лицензий на образовательную деятельность и аккредитации образовательной организации, подтверждающей ее право выдавать документы государственного образца по окончании учебы обучающимся.
- **нарушение договора** - неспособность клиента выполнять договорные обязательства связанные с продолжением обучения и оплатой за него, что влечет финансовые потери;
- **опасность для персонала/безопасность пользователей** - опасность кражи и неправомерного использования авторских научных трудов, образовательного контента, методических материалов, курсовых, дипломных, магистерских работ;
- **вторжение в частную жизнь пользователей** – кража и распространение персональных данных пользователей системы дистанционного обучения;
- **финансовые потери, связанные с чрезвычайными обстоятельствами или ремонтом** – (взлом системы дистанционного обучения, DoS- атаки, выход из строя электронных носителей, хранилищ информации, коммуникационного оборудования, отсутствие квалифицированного персонала на момент возникновения чрезвычайной ситуации);

- **потеря товаров/фондов/активов** – кража и незаконное использование конкурентами электронных образовательных ресурсов;
- **потеря клиентов-** в следствии неэффективной работы маркетинговых служб по своевременному и широкому распространению рекламной информации, проведению информационных акций и конкурсов;
- **судебные дела и штрафы** – размещение в системе дистанционного обучения контента противоречащего законадательству РФ и нарушение авторских прав при использовании электронных образовательных ресурсов;
- **потеря конкурентного преимущества** – необходимо использовать современные методики обучения и регулярно обновлять электронные образовательные ресурсы;
- **потеря технологического/технического лидерства** – необходимо следить за обновлением IT- инфраструктуры, соответствия ее производительности и объемов памяти требованиям для обслуживания большого количества сеансов одновременной работы с современными образовательными ресурсами в режиме реального времени;
- **потеря эффективности/надежности** – необходимо следить за повышением квалификации персонала системы дистанционного обучения, регулярно отслеживать необходимость обновления аппаратных средств, необходимо регулярно обновлять антивирусные программные средства, отслеживать DoS-атаки и использовать эффективные средства противодействия им;
- **потеря технической репутации** – необходимо следить за тем, чтобы не было регулярных сбоев оборудования, отказе в доступе к системе дистанционного обучения и сайту образовательной организации;
- **материальный ущерб** – кража оборудования, обслуживающего систему дистанционного обучения.

3) Шкала

Определим шкалу, которую будем использоваться в образовательной организации. Как правило, используется любое число уровней от 3 (например, низкий, средний и высокий) до 10 в соответствии с выбранным организацией подходом, для процесса оценки риска.

Образовательная организация в силу своего рода деятельности может установить собственные пределы ценности активов, такие, как «высокий», «средний», «низкий». Эти пределы оцениваться в соответствии с выбранными критериями (для возможных финансовых потерь пределы должны быть указаны в денежном выражении, при рассмотрении угрозы личной безопасности, определить денежную ценность может быть затруднительно и неприемлемо). Решение, что считать незначительными или серьезными последствиями, полностью зависит от организации.

Для системы дистанционного обучения выберем шкалу ценности актива от 0 до 4.

4) Зависимости

Чем более значимые и многочисленные бизнес-процессы поддерживаются активом, тем больше ценность этого актива. Должна быть также определена зависимость одних активов от других, поскольку это может влиять на ценность активов.

Информация о зависимостях поможет в определении угроз и особенно в выявлении уязвимостей. Кроме того, это поможет обеспечить правильное присвоение значения ценности активам (благодаря зависимым взаимосвязям), показывая, таким образом, соответствующий уровень защиты.

Ценность активов, от которых зависят другие активы, может изменяться следующим образом:

- если ценность зависимых активов (например, данных) ниже или равна ценности рассматриваемого актива (например, программного обеспечения), его ценность остается такой же;

- если ценность зависимых активов (например, данных) выше ценности рассматриваемого актива (например, программного обеспечения), его ценность должна быть увеличена в соответствии со степенью зависимости или ценностью других активов.

5) Результат

Окончательным результатом этого шага будет перечень активов и их ценности по отношению к модификации (сохранение целостности, подлинности, неотказуемости и учетности) раскрытию (сохранение конфиденциальности), разрушению и недоступности (сохранение надежности и доступности) и восстановительной стоимости.

Тип актива	**Активы**	**Ценность актива**
Основные активы		
Процесс	Процесс поступления-приема на дистанционную форму обучения. Процесс формирования образовательного контента. Процесс получения обучающимся образовательных материалов. Процесс дистанционного оказания обучающемуся консультационных услуг. Процесс отчетности обучающегося и оценка работы обучающегося. Процесс перевода обучающегося на следующий образовательный этап. Процессы маркетинга и обслуживания сайта образовательной организации и системы дистанционного обучения.	**4**
Информация	Информация о персональных данных учащихся и персонала системы дистанционного обучения. Информация о финансовом состоянии организации, предоставляющей услугу дистанционного получения образования. Информационные ресурсы базы данных образовательных электронных курсов	**3**
Вспомогательные активы		
Аппаратные средства	Серверы, персональные электронные устройства с доступом в сеть Интернет.	4

Программные средства	Операционная система. Антивирусные средства. Программная среда для организации дистанционного обучения на основе Moodle. Браузеры и плагины к ним для доступа к среде дистанционного обучения.	2
Сеть	Телекоммуникационные устройства, используемые для соединения нескольких физически удаленных компьютеров или элементов информационной системы. Устройства, являющиеся не оконечными, а промежуточными устройствами связи. Ретрансляторы, мосты, маршрутизаторы, коммутаторы, концентраторы. Сетевое программное обеспечение управления и мониторинга активного сетевого оборудования. Генерация журналов регистрации.	3
Персонал	Администрация организации осуществляющей дистанционную образовательную деятельность. Профессорско-преподавательский состав. Менеджеры дистанционного образовательного процесса, специалисты учебной части, методисты, разработчики образовательного контента и контента сайта образовательной организации. Руководитель отдела кадров, руководитель финансового отдела, руководитель, осуществляющий менеджмент риска. Персонал по эксплуатации и сопровождению информационной системы. Разработчики программных элементов среды дистанционного обучения и сайта образовательной организации.	3
Место функционирования организации	Офис и серверная. Внешний хостинг сайта. Удаленные точки доступа к системе дистанционного обучения.	1
Организация	Организация оказывающая образовательные услуги. Структура организации: Администрация. Кафедры. Организационно-методический отдел. Отдел маркетинга. IT-отдел. Бухгалтерия.	2

3.3.2 Определение угроз и источников угроз

Входные данные. Информация об угрозах, которая получена в результате анализа инцидента от владельцев активов, пользователей системы дистанционного обучения и из других источников, в том числе и списки внешних угроз.

Действие. Угрозы и их источники должны быть определены.

Руководство по реализации. Угроза может причинить ущерб активам организации, таким как информация, процессы и системы.

Угрозы могут быть умышленными, случайными или связанными с внешней средой (природными) и могут в результате представлять ущерб или потерю важных сервисов.

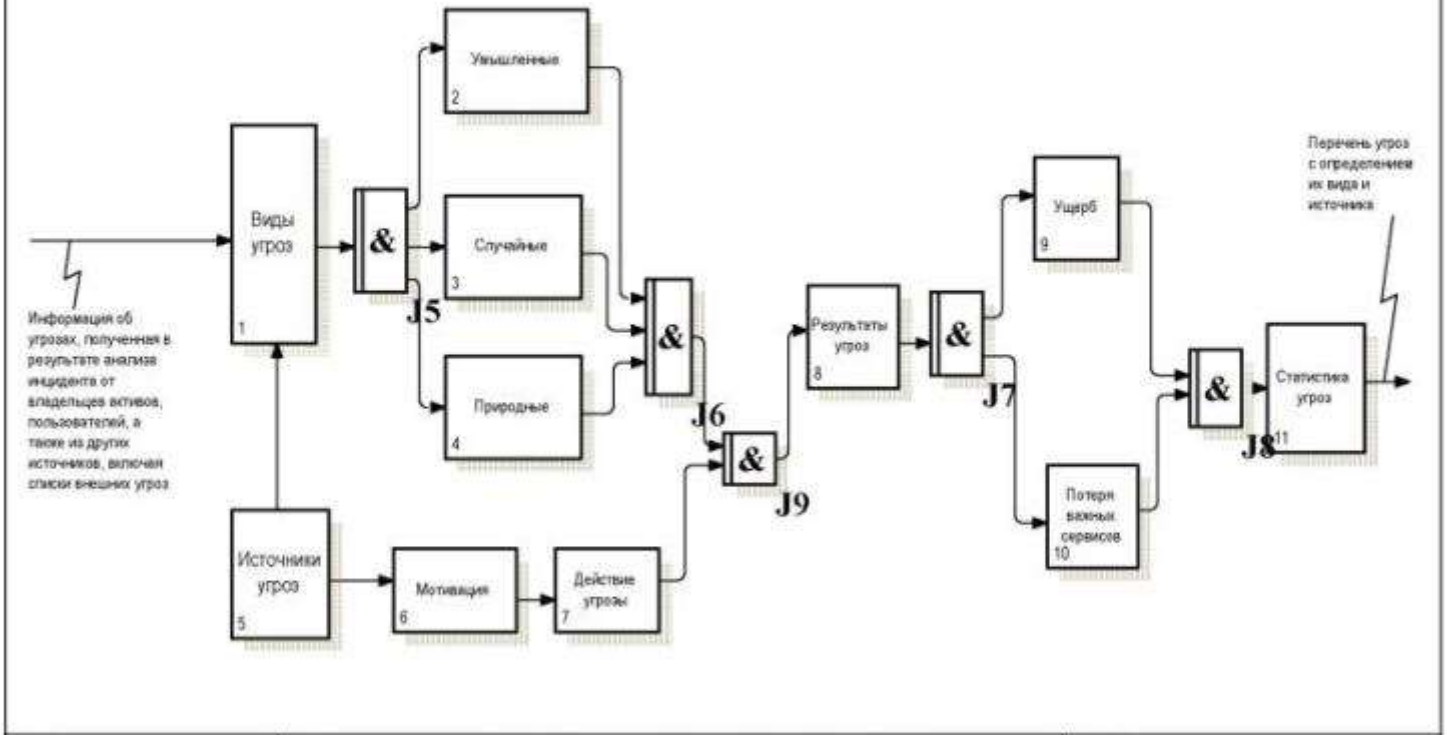
Необходимо установить случайные, преднамеренные, природные источники угроз. Угрозы могут исходить как из самой организации, так и из источника вне ее пределов. Угрозы должны определяться и в общем и по виду (это могут быть физический ущерб, неавторизованные действия, технические сбои), а затем, где это возможно, отдельные угрозы определяются внутри родового класса. Некоторые угрозы могут влиять более чем на один актив. В этих случаях они могут быть причиной различных влияний в зависимости от того, какие активы оказываются подвержены воздействию.

Входные данные для определения и количественной оценки вероятности возникновения угроз могут быть получены от владельцев активов или руководства организации, пользователей, персонала отдела кадров, специалистов в области ИБ, специалистов юридического отдела, экспертов в области физической безопасности, и других подразделений, а также от метеорологических служб, юридических организаций, национальных правительственных учреждений, страховых компаний. В ходе анализа угроз нужно учитывать аспекты среды и культуры.

Списки угроз и их статистику можно получить от федерального правительства, промышленных предприятий, страховых компаний, юридических организаций, и т.д.

Выходные данные этапа определения угроз и источников угроз. Перечень угроз с определением их вида и источника.

USED AT:	AUTHOR: Бечаров М.И.	DATE: 09.06.2014	WORKING	READER	DATE	CONTEXT:
	PROJECT: Оценка риска информационной безопасности	REV: 15.06.2014	DRAFT			TOP
	NOTES: 1 2 3 4 5 6 7 8 9 10		RECOMMENDED			
			PUBLICATION			



NODE:	TITLE:	NUMBER:
1	Определение угроз и их источников	5

В процессе оценки угроз в системе дистанционного обучения получен перечень угроз систематизированный по видам угроз в таблице 3.2.

Для каждой угрозы указывается ее происхождение: «П» (природная) «У» (умышленная), «С» (случайная), угроза.

- «П» обозначает все инциденты, не основанные на действиях персонала.
- «У» обозначает все умышленные действия, направленные на информационные активы.
- «С» обозначает все действия персонала, которые могут случайно нанести ущерб информационным активам.

Угрозы перечисляются не в приоритетном порядке.

Таблица 3.2

Перечень угроз системе дистанционного обучения

Вид	Угрозы	Происхождение
Физический ущерб	Пожар	С, У, П
	Ущерб, причиненный водой	С, У, П
	Разрушение оборудования или носителей	С, У, П
	Пыль, коррозия, замерзание	С, У, П
Природные явления	Климатическое явление	П
	Метеорологическое явление	П
Утрата важных сервисов	Авария системы кондиционирования воздуха или водоснабжения	С, У
	Нарушение энергоснабжения	С, У, П
	Отказ телекоммуникационного оборудования	С, У
Помехи вследствие излучения	Электромагнитное излучение	С, У, П
	Тепловое излучение	С, У, П
	Электромагнитные импульсы	С, У, П
Компрометация информации	Перехват компрометирующих сигналов помех	У
	Кража носителей или документов	У
	Кража оборудования	У
	Раскрытие	С, У
	Данные из ненадежных источников	С, У

Вид	Угрозы	Происхождение
	Преступное использование аппаратных средств	У
	Преступное использование программного обеспечения	С, У
	Определение местонахождения	У
Технические неисправности	Отказ оборудования	С
	Неисправная работа оборудования	С
	Насыщение информационной системы	С, У
	Нарушение функционирования программного обеспечения	С
	Нарушение сопровождения информационной системы	С, У
Несанкционированные действия	Несанкционированное использование оборудования	У
	Мошенническое копирование программного обеспечения	У
	Использование контрафактного или скопированного программного обеспечения	С, У
	Искажение данных	У
	Незаконная обработка данных	У
Компрометация функций	Ошибка при использовании	С
	Злоупотребление правами	С, У
	Фальсификация прав	У
	Отказ в осуществлении действий	У
	Нарушение работоспособности персонала	С, У, П

Источники угроз, происходящие от деятельности человека.

Таблица3.3

Источники угрозы системе дистанционного обучения

Источник угрозы	Мотивация	Действие угрозы
Хакер, взломщик	Вызов Самомнение Бунтарство Статус Деньги	Хакерство Социальная инженерия Проникновение в систему, взлом Несанкционированный доступ к системе
Лицо, совершающее компьютерное преступление	Разрушение информации Незаконное раскрытие информации Денежная выгода Несанкционированное изменение данных	Компьютерное преступление (компьютерное преследование и др. действия) Мошенническая деятельность (воспроизведение, выдача себя за другого, перехват и др. действия) Информационный подкуп Получение доступа обманным путем

Источник угрозы	Мотивация	Действие угрозы
		Проникновение в систему
Террорист	Шантаж Разрушение Использование в личных интересах Месть Политическая выгода Охват среды (передачи данных)	Взрыв/Терроризм Информационная война Системная атака (распределенный отказ в обслуживании, DoS-атаки и др. действия) Проникновение в систему Порча системы
Промышленный шпионаж (сведения секретного характера компании)	Конкурентное преимущество Экономический шпионаж	Получение информационного преимущества Экономическая эксплуатация Хищение информации Покушение на неприкосновенность личной жизни Социальная инженерия Проникновение в систему Несанкционированный доступ к системе (доступ к секретной информации, являющейся собственностью фирмы и/или связанной с технологией)
Инсайдеры (плохо обученные, недовольные, злонамеренные, беспечные, нечестные или уволенные служащие)	Любопытство Самомнение Разведка Денежная выгода Месть Ненамеренные ошибки и упущения (например, ошибка ввода данных, ошибка в составлении программы)	Нападение на служащего Шантаж Просмотр информации, являющейся собственностью фирмы Неправильное использование компьютера Мошенничество и хищение Информационный подкуп Вредоносное программное обеспечение (например вирус, логическая бомба, Троянский конь) Продажа информации личного характера «Жучки» в системе Проникновение в систему Вредительство в системе Несанкционированный доступ к системе

3.3.3 Определение существующих мер и средств контроля и управления

Входные данные. Документация по мерам и средствам контроля и управления и планы по реализации обработки риска.

Действие. Определяются существующие и планируемые меры и средства контроля и управления.

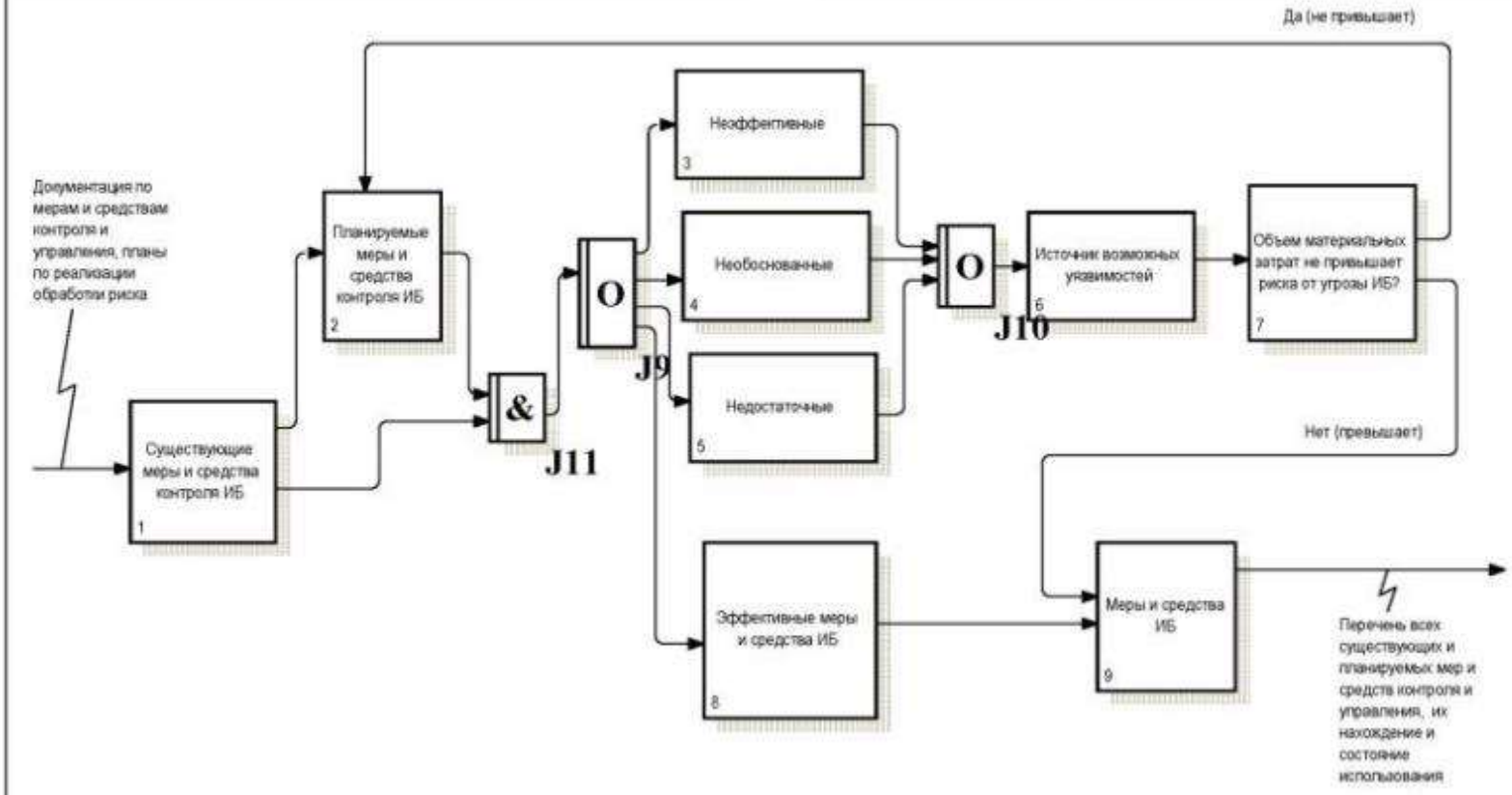
Руководство по реализации. Во избежание лишней работы или расходов, например, при дублировании мер и средств контроля и управления, необходимо определить существующие меры и средства контроля и управления. Помимо этого, при определении существующих мер и средств контроля и управления необходимо провести проверку, чтобы убедиться в правильности функционирования мер и средств контроля и управления – процедура обращения к существующим отчетам по аудиту системы менеджмента ИБ должна сокращать время, затрачиваемое на решение этой задачи. Ненадлежащее функционирование средств и мер управления и контроля может стать причиной уязвимости.

Один из способов количественной оценки действия средств и мер управления и контроля - выявить, то как снижается вероятность возникновения угрозы, затрудняется использование уязвимости и возможности влияния инцидента. Проверки, проводимые руководством, и отчеты по аудиту также обеспечивают информацию об эффективности существующих мер и средств контроля и управления.

Существующие или планируемые меры и средства контроля и управления могут быть отнесены к разряду неэффективных, недостаточных или необоснованных. Если их отнесли к необоснованным или недостаточным, средство и меру контроля и управления необходимо подвергнуть проверке, чтобы определить, подлежат ли они замене более подходящими, удалению, или возможно стоит оставить их по причине стоимости.

Выходные данные. Перечень всех существующих и планируемых мер и средств контроля и управления, их нахождение и состояние использования.

USED AT:	AUTHOR: Бочаров М.И.	DATE: 09.06.2014	■	WORKING	READER	DATE	CONTEXT:
	PROJECT: Оценка риска информационной безопасности	REV: 15.06.2014		DRAFT			TOP
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			



NODE:	TITLE:	NUMBER:
1	Определение существующих мер и средств контроля и управления ИБ	6

Меры и средства контроля и управления обеспечения ИБ системы дистанционного обучения:

- документирование процессов менеджмента ИБ с целью доступности информации о всех существующих или планируемых мерах и средствах контроля и управления, а также о состоянии их реализации.

- регулярный анализ документов, содержащих информацию о средствах контроля и управления в том числе планов обработки рисков.

- проверки, проводимые совместно с сотрудниками, отвечающими за ИБ (представителем администрации, сотрудником обеспечивающем ИБ в целом, сотрудником, отвечающим за безопасность программной системы дистанционного обучения, охраной офиса здания, представителями профессорско-преподавательского состава и представителями пользователей системы);

- регулярный обход здания и осмотр физических средств контроля, сравнение существующих средств контроля с документированным списком средств, проверка существующих средств контроля на их правильную и эффективную работу;

- анализ результатов внутренних аудитов.

3.3.4 Выявление уязвимостей информационной безопасности

Входные данные. Перечни известных угроз, перечни активов и существующих мер и средств контроля и управления.

Действие. Необходимо выявить уязвимости, которые могут быть использованы угрозами для нанесения ущерба активам или организации.

Руководство по реализации. Уязвимости могут быть выявлены в следующих областях:

- организация работ;
- установившийся порядок управления;
- процессы и процедуры;
- персонал;

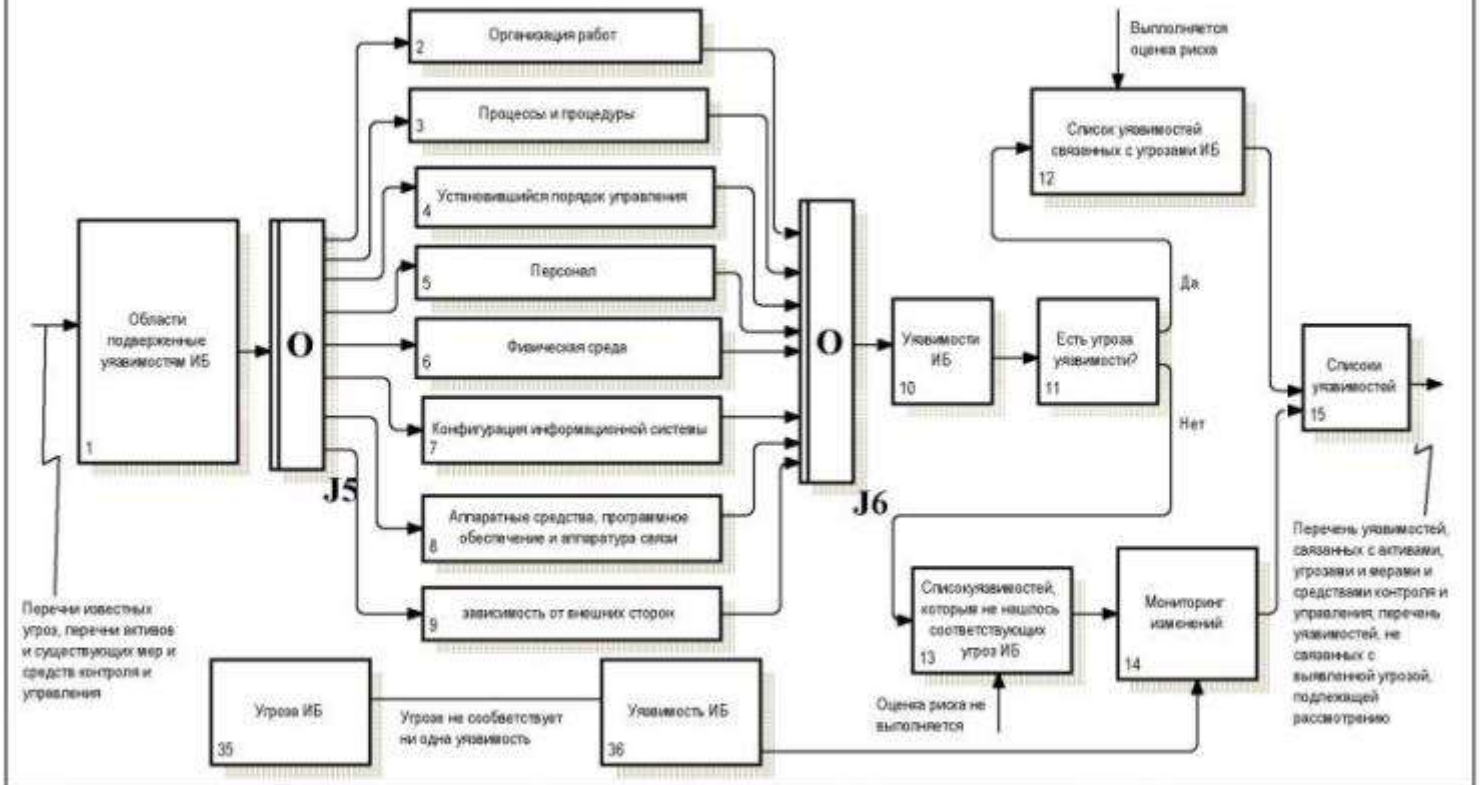
- конфигурация информационной системы;
- физическая среда;
- аппаратные средства, программное обеспечение и аппаратура связи;
- зависимость от внешних сторон.

Наличие уязвимости не наносит ущерба само по себе, так как необходимо наличие угрозы, которая сможет воспользоваться уязвимостью. Для уязвимости, которой не соответствует определенная угроза, может не потребоваться внедрение средства контроля и управления, но она должна осознаваться, учитываться и подвергаться мониторингу на предмет изменений. С другой стороны, угроза, которой не соответствует определенная уязвимость, может не приводить к риску. Неверно реализованное, неправильно используемое, неправильно функционирующее средство управления и контроля само может стать причиной уязвимости. Эффективность или неэффективность мер и средств управления и контроля может зависить от среды, в которой они функционируют.

Уязвимости могут быть связаны со свойствами актива, так как способ и цели использования актива в процессе оказания образовательной услуги могут отличаться от планируемых при приобретении или создании актива. Нужно учитывать уязвимости, возникающие из разных источников, и которые являются внешними и внутренние по отношению к активу.

Выходные данные. Перечень уязвимостей, связанных с активами, угрозами и мерами и средствами контроля и управления; перечень уязвимостей, не связанных с выявленной угрозой, подлежащей рассмотрению.

USED AT:	AUTHOR: Бечаров М.И.	DATE: 09.06.2014	WORKING	READER: DATE	CONTEXT:
	PROJECT: Оценка риска информационной безопасности	REV: 15.06.2014	DRAFT		TOP
	NOTES: 1 2 3 4 5 6 7 8 9 10		RECOMMENDED		
			PUBLICATION		



NODE:	TITLE:	NUMBER:
1	Выявление уязвимостей ИБ	7

Уязвимости и методы оценки уязвимости

Таблица 3.4

Уязвимости ИБ и соответствующие им угрозы для системы дистанционного обучения

Вид	Уязвимости ИБ	Угрозы ИБ
Аппаратные средства	Недостаточное техническое обслуживание/неправильная установка носителей данных	Нарушение ремонтопригодности информационных систем
	Отсутствие программ периодической замены	Ухудшение состояния носителей данных
	Чувствительность к влажности, пыли, загрязнению	Образование пыли, коррозия, замерзание
	Чувствительность к электромагнитному излучению	Электромагнитное излучение
	Отсутствие эффективного контроля изменений конфигурации	Ошибка в использовании
	Чувствительность к колебаниям напряжения	Потеря электропитания
	Чувствительность к колебаниям температуры	Метеорологические явления
	Незащищенное хранение	Хищение носителей данных или документов
	Небрежное (безответственное) размещение	Хищение носителей данных или документов
	Неконтролируемое копирование	Хищение носителей данных или документов
Программные средства	Отсутствующее или недостаточное тестирование программных средств	Злоупотребление правами
	Широко известные дефекты программных средств	Злоупотребление правами
	Отсутствие «завершения сеанса» при уходе с рабочего места	Злоупотребление правами
	Списание или повторное использование носителей данных без надлежащего удаления информации	Злоупотребление правами
	Отсутствие «следов» аудита	Злоупотребление правами
	Неверное распределение прав доступа	Злоупотребление правами
	Широко распределенное программное обеспечение	Порча данных

Вид	Уязвимости ИБ	Угрозы ИБ
	Применение прикладных программ для несоответствующих, с точки зрения времени, данных	Порча данных
	Сложный пользовательский интерфейс	Ошибка в использовании
	Отсутствие документации	Ошибка в использовании
	Неправильные параметры установки	Ошибка в использовании
	Неправильные данные	Ошибка в использовании
	Отсутствие механизмов идентификации и аутентификации, таких, как аутентификация пользователей	Фальсификация прав
	Незащищенные таблицы паролей	Фальсификация прав
	Плохой менеджмент паролей	Фальсификация прав
	Активизация ненужных сервисов	Нелегальная обработка данных
	Недоработанное или новое программное обеспечение	Сбой программных средств
	Нечеткие или неполные спецификации для разработчиков	Сбой программных средств
	Отсутствие эффективного контроля изменений	Сбой программных средств
	Неконтролируемая загрузка и использование программных средств	Тайные действия с программными средствами
	Отсутствие резервных копий	Тайные действия с программными средствами
	Отсутствие физической защиты здания, дверей и окон	Хищение носителей данных или документов
	Отказ в обеспечении отчетов по менеджменту	Неавторизованное использование оборудования
Сеть	Отсутствие подтверждения отправления или получения сообщения	Отказ в осуществлении действий
	Незащищенные линии связи	Перехват информации
	Незащищенный чувствительный трафик	Перехват информации
	Плохая разводка кабелей	Отказ телекоммуникационного оборудования
	Единая точка отказа	Отказ телекоммуникационного оборудования
	Отсутствие идентификации и аутентификации отправителя и получателя	Фальсификация прав
	Ненадежная сетевая архитектура	Дистанционный шпионаж
	Передача паролей в незашифрованном виде	Дистанционный шпионаж
	Неадекватный сетевой менеджмент	Насыщение информационной

Вид	Уязвимости ИБ	Угрозы ИБ
	(устойчивость маршрутизации)	системы
	Незащищенные соединения сети общего пользования	Неавторизованное использование оборудования
Персонал	Отсутствие персонала	Нарушение работоспособности персонала
	Неадекватные процедуры набора персонала	Разрушение оборудования или носителей данных
	Недостаточное осознание безопасности	Ошибка в использовании
	Ненадлежащее использование программных и аппаратных средств	Ошибка в использовании
	Отсутствие осведомленности о безопасности	Ошибка в использовании
	Отсутствие механизмов мониторинга	Нелегальная обработка данных
	Безнадзорная работа внешнего персонала или персонала организации, занимающегося уборкой	Хищение носителей данных или документов
	Отсутствие политик по правильному использованию телекоммуникационной среды и обмена сообщениями	Неавторизованное использование оборудования
Место функционирования организации	Неадекватное или небрежное использование физического управления доступом к зданиям и помещениям	Ухудшение состояния носителей данных
	Размещение в местности, предрасположенной к наводнениям	Затопление
	Нестабильная электрическая сеть	Отсутствие электропитания
	Отсутствие физической защиты здания, дверей и окон	Хищение аппаратуры
Организация	Отсутствие формальной процедуры для регистрации и снятия с регистрации пользователей	Злоупотребление правами
	Отсутствие формального процесса для пересмотра (надзора) прав доступа	Злоупотребление правами
	Отсутствие или недостаточные условия (касающиеся безопасности) в договорах с клиентами и/или третьими сторонами	Злоупотребление правами
	Отсутствие процедуры, касающейся мониторинга средств обработки информации	Злоупотребление правами
	Отсутствие регулярных аудитов (надзора)	Злоупотребление правами
	Отсутствие процедур идентификации и оценки риска	Злоупотребление правами
	Отсутствие сообщений об ошибках,	Злоупотребление правами

Вид	Уязвимости ИБ	Угрозы ИБ
	зафиксированных в журнале регистрации администратора и оператора	
	Неадекватная ответственность за техническое обслуживание	Нарушение обслуживания информационной системы
	Отсутствующее или неудовлетворительное соглашение об уровне сервиса	Нарушение обслуживания информационной системы
	Отсутствие процедуры контроля изменений	Нарушение обслуживания информационной системы
	Отсутствие формальной процедуры контроля документации, касающейся системы менеджмента ИБ	Порча данных
	Отсутствие формальной процедуры надзора за записями системы менеджмента ИБ	Порча данных
	Отсутствие формального процесса санкционирования общедоступной информации	Данные из ненадежных источников
	Отсутствие надлежащего распределения обязанностей по обеспечению информационной безопасности	Отказ в осуществлении деятельности
	Отсутствие планов обеспечения непрерывности бизнеса	Отказ оборудования
	Отсутствие политики по использованию электронной почты	Ошибка в использовании
	Отсутствие процедур введения программного обеспечения в операционные системы	Ошибка в использовании
	Отсутствие записей в журнале регистрации администратора и оператора	Ошибка в использовании
	Отсутствие процедур для обработки секретной информации	Ошибка в использовании
	Отсутствие обязанностей по обеспечению информационной безопасности в должностных инструкциях	Ошибка в использовании
	Отсутствие или недостаточные условия (касающиеся информационной безопасности) в договорах со служащими	Нелегальная обработка данных
	Отсутствие оговоренного дисциплинарного процесса в случае инцидента безопасности	Хищение оборудования
	Отсутствие формальной политики по использованию портативных компьютеров	Хищение оборудования
	Отсутствие контроля над активами,	Хищение оборудования

Вид	Уязвимости ИБ	Угрозы ИБ
	находящимися за пределами организации	
	Отсутствующая или неудовлетворительная политика «чистого стола и пустого экрана»	Хищение носителей информации или документов
	Отсутствие авторизации средств обработки информации	Хищение носителей информации или документов
	Отсутствие установленных механизмов мониторинга нарушений безопасности	Хищение носителей информации или документов
	Отсутствие регулярных проверок, проводимых руководством	Неавторизованное использование оборудования
	Отсутствие процедур сообщения о слабых местах безопасности	Неавторизованное использование оборудования
	Отсутствие процедур, обеспечивающих соблюдение прав на интеллектуальную собственность	Использование контрафактных или копированных программных средств

3.3.5 Определение последствий

Входные данные. Перечень активов, бизнес-процессов, угроз и уязвимостей, где это уместно, связанных с активами, и их значимость.

Действие. Должны быть определены последствия для активов, вызванные потерей конфиденциальности, целостности и доступности.

Руководство по реализации. Последствием может быть снижение эффективности, неблагоприятные операционные условия, потеря бизнеса, ущерб, нанесенный репутации и т.д.

Эта деятельность определяет ущерб или последствия для организации, которые могут быть обусловлены сценарием инцидента. Сценарий инцидента - это описание угрозы, использующей определенную уязвимость или совокупность уязвимостей в инциденте информационной безопасности. Влияние сценариев инцидентов обусловливается критериями влияния, определяемыми в ходе деятельности по установлению контекста. Влияние может затрагивать один или несколько активов, а также часть актива. Поэтому активам может назначаться ценность, обусловленная как их финансовой стоимостью, так и последствиями для бизнеса в случае их порчи

или компрометации. Последствия могут быть временными или постоянными, как это бывает в случае разрушения активов.

Организации должны определять операционные последствия сценариев инцидентов на основе (но не ограничиваясь):

- времени на расследование и восстановление;
- потерь (рабочего) времени;
- упущенной возможности;
- охраны труда и безопасности;
- финансовых затрат на приобретение специфических навыков, необходимых для устранения неисправности;
- репутации и иного «неосязаемого капитала».

Оценка влияния

Инцидент ИБ может оказывать влияние более чем на один актив или только на часть актива. Влияние связано со степенью успешности инцидента. Как следствие, существует важное различие между ценностью актива и влиянием, являющимся результатом инцидента. Влияние рассматривается как имеющее либо незамедлительный (операционный) эффект, либо будущий (бизнес-) эффект, который включает финансовые и рыночные последствия.

Непосредственное (операционное) влияние бывает прямым или косвенным.

Прямое влияние:

- финансовая восстановительная стоимость потерянного актива (части актива);
- стоимость приостановленных из-за инцидента операций, пока услуга, предоставляемая активом (активами), не будет восстановлена;
- стоимость приобретения, конфигурирования и установки нового актива или резервной копии;
- влияние приводит к нарушению ИБ.

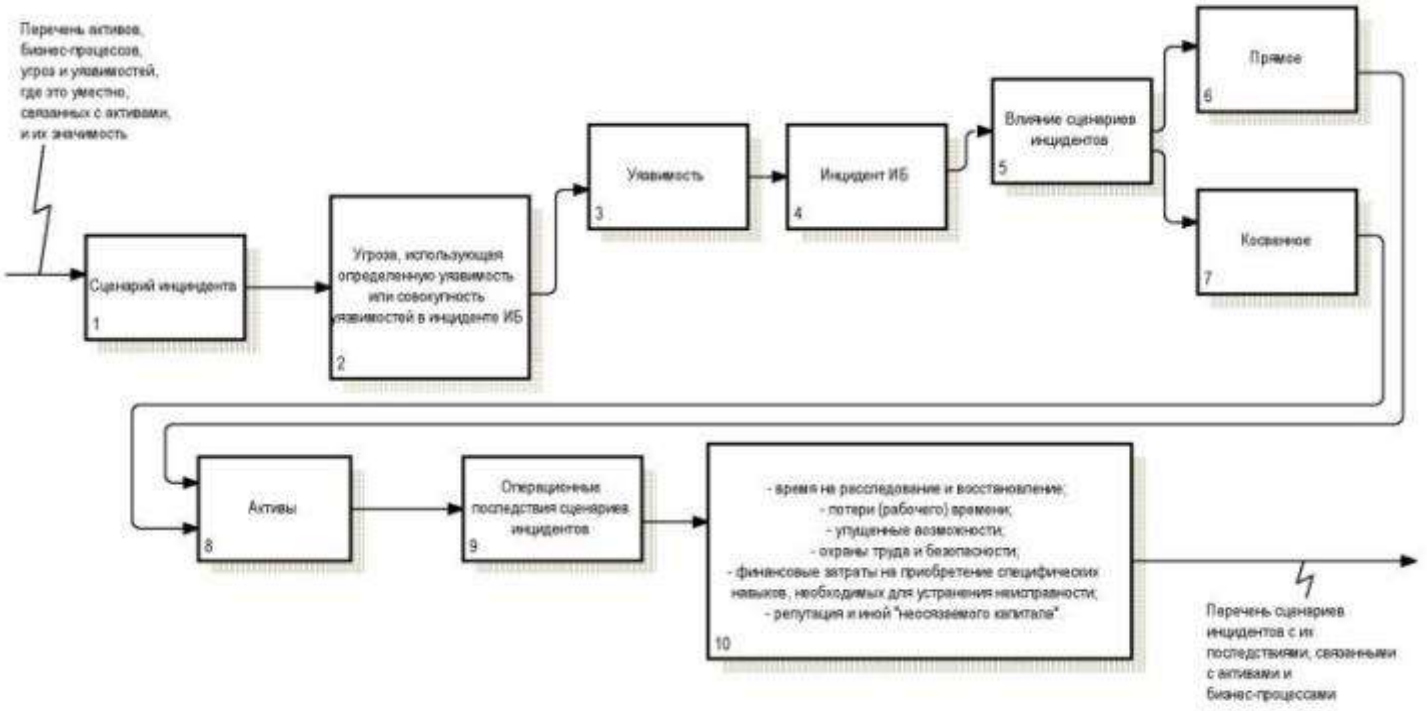
Косвенное влияние:

- стоимость прерванных операций;
- издержки упущенных возможностей (финансовые ресурсы, необходимые для замены или восстановления актива, могли быть использованы где-либо еще);
- возможное злоупотребление информацией, полученной в результате нарушения безопасности;
- нарушение этических норм поведения;
- нарушение установленных законом или нормативных обязательств.

Первая оценка (без мер и средств контроля и управления любого рода) будет оценивать влияние как очень близкое к ценности связанного с этим актива или комбинации активов. При каждой последующей итерации для этого (этих) актива (активов) влияние будет отличаться (обычно будет гораздо ниже) вследствие наличия и эффективности реализованных мер и средств контроля и управления.

Выходные данные. Перечень сценариев инцидентов с их последствиями, связанными с активами и бизнес-процессами.

USED AT:	AUTHOR: Бечаров М.И.	DATE: 09.06.2014		WORKING	READER	DATE	CONTEXT:
	PROJECT: Оценка риска информационной безопасности	REV: 16.06.2014		DRAFT			TOP
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			



NODE:	TITLE:	NUMBER:
1	Определение последствий для активов, вызванных потерей конфиденциальности, целостности и доступности	8

Таблица 3.5

Перечень сценариев инцидентов с их последствиями, связанными с активами и бизнес-процессами.

Перечень сценариев инцидентов	Угроза использующая уязвимость	Уязвимость	Активы и бизнес процессы	Операционные последствия сценариев
С аппаратными средствами	Нарушение ремонтопригодности информационных систем	Недостаточное техническое обслуживание/неправильная установка носителей данных	Серверы, персональные электронные устройства с доступом в сеть Интернет.	- время на расследование и восстановление; - потери (рабочего) времени; - упущенные возможности; - репутация и иной «неосязаемого капитала».
	Ухудшение состояния носителей данных	Отсутствие программ периодической замены		
	Образование пыли, коррозия, замерзание	Чувствительность к влажности, пыли, загрязнению		
	Электромагнитное излучение	Чувствительность к электромагнитному излучению		
	Ошибка в использовании	Отсутствие эффективного контроля изменений конфигурации		
	Потеря электропитания	Чувствительность к колебаниям напряжения		
	Метеорологические явления	Чувствительность к колебаниям температуры		
	Хищение носителей данных или документов	Незащищенное хранение		
		Небрежное (безответственное) размещение		
		Неконтролируемое копирование		
С программными средствами	Злоупотребление правами	Отсутствующее или недостаточное тестирование программных средств	Операционная система. Антивирусные средства. Программная среда для организации дистанционного	- время на расследование и восстановление; - потери (рабочего) времени; - упущенные
		Широко известные дефекты программных средств		
		Отсутствие «завершения сеанса» при уходе с рабочего места		
		Списание или повторное использование носителей данных без надлежащего удаления информации		

Перечень сценариев инцидентов	Угроза использующая уязвимость	Уязвимость	Активы и бизнес процессы	Операционные последствия сценариев
		Отсутствие «следов» аудита	обучения на основе Moodle. Браузеры и плагины к ним для доступа к среде дистанционного обучения.	возможности; - охраны труда и безопасности; - финансовые затраты на приобретение специфических навыков, необходимых для устранения неисправности; - репутация и иной «неосязаемого капитала».
		Неверное распределение прав доступа		
	Порча данных	Широко распределенное программное обеспечение		
		Применение прикладных программ для несоответствующих, с точки зрения времени, данных		
	Ошибка в использовании	Сложный пользовательский интерфейс		
		Отсутствие документации		
		Неправильные параметры установки		
		Неправильные данные		
	Фальсификация прав	Отсутствие механизмов идентификации и аутентификации, таких, как аутентификация пользователей		
		Незащищенные таблицы паролей		
		Плохой менеджмент паролей		
	Нелегальная обработка данных	Активизация ненужных сервисов		
	Сбой программных средств	Недоработанное или новое программное обеспечение		
		Нечеткие или неполные спецификации для разработчиков		
		Отсутствие эффективного контроля изменений		
	Тайные действия с программными средствами	Неконтролируемая загрузка и использование программных средств		
		Отсутствие резервных копий		
	Хищение носителей данных или документов	Отсутствие физической защиты здания, дверей и окон		
	Неавторизованное использование оборудования	Отказ в обеспечении отчетов по менеджменту		

Перечень сценариев инцидентов	Угроза использующая уязвимость	Уязвимость	Активы и бизнес процессы	Операционные последствия сценариев
С сетью	Отказ в осуществлении действий	Отсутствие подтверждения отправления или получения сообщения	Телекоммуникационные устройства, используемые для соединения нескольких физически удаленных компьютеров или элементов информационной системы. Устройства, являющиеся не оконечными, а промежуточными устройствами связи. Ретрансляторы, мосты, маршрутизаторы, коммутаторы, концентраторы. Сетевое программное обеспечение управления и мониторинга активного сетевого оборудования. Генерация журналов регистрации.	- время на расследование и восстановление; - потери (рабочего) времени; - упущенные возможности; - охраны труда и безопасности; - финансовые затраты на приобретение специфических навыков, необходимых для устранения неисправности; - репутация и иной «неосязаемого капитала».
	Перехват информации	Незащищенные линии связи		
		Незащищенный чувствительный трафик		
	Отказ телекоммуникационного оборудования	Плохая разводка кабелей		
		Единая точка отказа		
	Фальсификация прав	Отсутствие идентификации и аутентификации отправителя и получателя		
	Дистанционный шпионаж	Ненадежная сетевая архитектура		
		Передача паролей в незашифрованном виде		
	Насыщение информационной системы	Неадекватный сетевой менеджмент (устойчивость маршрутизации)		
	Неавторизованное использование оборудования	Незащищенные соединения сети общего пользования		

Перечень сценариев инцидентов	Угроза использующая уязвимость	Уязвимость	Активы и бизнес процессы	Операционные последствия сценариев
С персоналом	Нарушение работоспособности персонала	Отсутствие персонала	Администрация организации осуществляющей дистанционную образовательную деятельность. Профессорско-преподавательский состав. Менеджеры дистанционного образовательного процесса, специалисты учебной части, методисты, разработчики образовательного контента и контента сайта образовательной организации. Руководитель отдела кадров, руководитель финансового отдела, руководитель, осуществляющий	- потери (рабочего) времени; - упущенные возможности; - охраны труда и безопасности; - финансовые затраты на приобретение специфических навыков, необходимых для устранения неисправности;
	Разрушение оборудования или носителей данных	Неадекватные процедуры набора персонала		
	Ошибка в использовании	Недостаточное осознание безопасности		
		Ненадлежащее использование программных и аппаратных средств		
		Отсутствие осведомленности о безопасности		
	Нелегальная обработка данных	Отсутствие механизмов мониторинга		
	Хищение носителей данных или документов	Безнадзорная работа внешнего персонала или персонала организации, занимающегося уборкой		
	Неавторизованное использование оборудования	Отсутствие политик по правильному использованию телекоммуникационной среды и обмена сообщениями		

Перечень сценариев инцидентов	Угроза использующая уязвимость	Уязвимость	Активы и бизнес процессы	Операционные последствия сценариев
			менеджмент риска. Персонал по эксплуатации и сопровождению информационной системы. Разработчики программных элементов среды дистанционного обучения и сайта образовательной организации.	
С местом функционирования организации	Ухудшение состояния носителей данных	Неадекватное или небрежное использование физического управления доступом к зданиям и помещениям	Офис и серверная. Внешний хостинг сайта. Удаленные точки доступа к системе дистанционного обучения.	- время на расследование и восстановление; - потери (рабочего) времени; - охраны труда и безопасности;
	Затопление	Размещение в местности, предрасположенной к наводнениям		
	Отсутствие электропитания	Нестабильная электрическая сеть		
	Хищение аппаратуры	Отсутствие физической защиты здания, дверей и окон		
С организацией	Злоупотребление правами	Отсутствие формальной процедуры для регистрации и снятия с регистрации пользователей	Организация оказывающая образовательные услуги. Структура организации:	- время на расследование и восстановление; - потери (рабочего) времени;
		Отсутствие формального процесса для пересмотра (надзора) прав доступа		
		Отсутствие или недостаточные условия (касающиеся		

Перечень сценариев инцидентов	Угроза использующая уязвимость	Уязвимость	Активы и бизнес процессы	Операционные последствия сценариев
		безопасности) в договорах с клиентами и/или третьими сторонами	Администрация. Кафедры. Организационно-методический отдел. Отдел маркетинга. IT-отдел. Бухгалтерия.	- упущенные возможности; - охраны труда и безопасности; - финансовые затраты на приобретение специфических навыков, необходимых для устранения неисправности; - репутация и иной «неосязаемого капитала».
		Отсутствие процедуры, касающейся мониторинга средств обработки информации		
		Отсутствие регулярных аудитов (надзора)		
		Отсутствие процедур идентификации и оценки риска		
		Отсутствие сообщений об ошибках, зафиксированных в журнале регистрации администратора и оператора		
	Нарушение обслуживания информационной системы	Неадекватная ответственность за техническое обслуживание		
		Отсутствующее или неудовлетворительное соглашение об уровне сервиса		
		Отсутствие процедуры контроля изменений		
	Порча данных	Отсутствие формальной процедуры контроля документации, касающейся системы менеджмента ИБ		
		Отсутствие формальной процедуры надзора за записями системы менеджмента ИБ		
	Данные из ненадежных источников	Отсутствие формального процесса санкционирования общедоступной информации		
	Отказ в осуществлении деятельности	Отсутствие надлежащего распределения обязанностей по обеспечению информационной безопасности		
	Отказ оборудования	Отсутствие планов обеспечения непрерывности бизнеса		
	Ошибка в использовании	Отсутствие политики по использованию электронной почты		
		Отсутствие процедур введения программного обеспечения в операционные системы		

Перечень сценариев инцидентов	Угроза использующая уязвимость	Уязвимость	Активы и бизнес процессы	Операционные последствия сценариев
		Отсутствие записей в журнале регистрации администратора и оператора		
		Отсутствие процедур для обработки секретной информации		
		Отсутствие обязанностей по обеспечению информационной безопасности в должностных инструкциях		
	Нелегальная обработка данных	Отсутствие или недостаточные условия (касающиеся информационной безопасности) в договорах со служащими		
	Хищение оборудования	Отсутствие оговоренного дисциплинарного процесса в случае инцидента безопасности		
		Отсутствие формальной политики по использованию портативных компьютеров		
		Отсутствие контроля над активами, находящимися за пределами организации		
	Хищение носителей информации или документов	Отсутствующая или неудовлетворительная политика «чистого стола и пустого экрана»		
		Отсутствие авторизации средств обработки информации		
		Отсутствие установленных механизмов мониторинга нарушений безопасности		
	Неавторизованное использование оборудования	Отсутствие регулярных проверок, проводимых руководством		
		Отсутствие процедур сообщения о слабых местах безопасности		
	Использование контрафактных или копированных	Отсутствие процедур, обеспечивающих соблюдение прав на интеллектуальную собственность		

Перечень сценариев инцидентов	Угроза использующая уязвимость	Уязвимость	Активы и бизнес процессы	Операционные последствия сценариев
	программных средств			

3.4 Анализ риска: установление значения риска

3.4.1 Методология установления значения риска

Методология установления значения риска может быть количественной, качественной, комбинированной, в зависимости от обстоятельств. Установление качественного значения часто используется вначале для получения общих сведений об уровне риска и выявления основных значений рисков. Позднее может возникнуть необходимость в осуществлении более специфичного установления количественного анализа основных значений рисков, поскольку обычно выполнение качественного анализа по сравнению с количественным является менее сложным и затратным.

Для установления качественного значения используется шкала квалификации атрибутов, с помощью которой описываются величины возможных последствий (например, низкий, средний и высокий) и вероятности возникновения этих последствий. Преимущество установления качественного значения заключается в доступности для понимания всем соответствующим персоналом, а недостатком - зависимость от субъективного выбора шкалы.

Для установления количественной оценки используется шкала с числовыми значениями (а не описательные шкалы, используемые при установлении качественного значения) как последствий, так и вероятности, с применением данных из различных источников. Качество анализа зависит от точности и полноты числовых значений и от обоснованности используемых моделей. В большинстве случаев для установления количественного значения используются фактические данные за прошедший период.

3.4.2 Оценка последствий

Входные данные. Перечень определенных значимых сценариев инцидентов, включая выявление угроз, уязвимостей и затронутых активов, а также последствий для активов и бизнес-процессов.

Действие. Должно быть оценено влияние на бизнес организации, которое может быть результатом предполагаемых или фактических инцидентов ИБ с учетом последствий нарушения ИБ, таких, как потеря конфиденциальности, целостности или доступности активов.

Руководство по реализации. После определения всех проверяемых активов, присвоенная им ценность должна учитываться при оценке последствий.

Значение влияния на бизнес может быть выражено в качественной или количественной формах.

Определение ценности активов начинается с классификации активов в соответствии с их критичностью с точки зрения важности активов для осуществления бизнес-целей организации. Затем ценность активов определяется с использованием двух мер:

- восстановительной стоимости актива - стоимости его очистки с целью восстановления и замены информации (если это возможно);
- последствий для бизнеса от потери или компрометации актива, например возможные неблагоприятные последствия для бизнеса и/или законодательные или регулирующие последствия раскрытия, модификации, недоступности и/или разрушения информации, а также других информационных активов.

Это определение ценности может быть установлено на основе анализа влияния на бизнес. Ценность, определяемая последствиями для бизнеса, обычно значительно выше просто восстановительной стоимости и зависит от значимости актива для организации при выполнении ее бизнес-целей.

Определение ценности активов является ключевым фактором оценки влияния сценария инцидента, поскольку инцидент может затрагивать более

одного актива (например, зависимые активы), или только часть актива. Различные угрозы и уязвимости могут иметь различное влияние на активы, например потеря конфиденциальности, целостности и доступности. Поэтому оценка последствий связана с определением ценности активов или становится связанной, исходя из анализа влияния на бизнес.

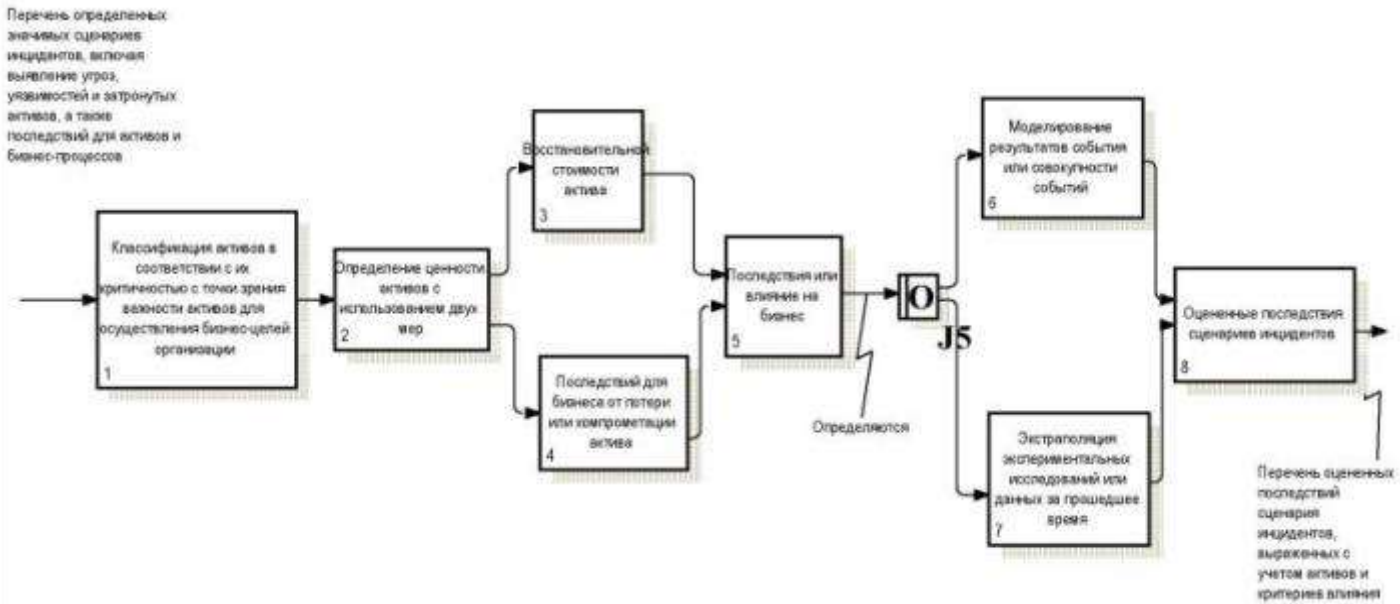
Последствия или влияние на бизнес могут определяться путем моделирования результатов события или совокупности событий, экстраполяции экспериментальных исследований или данных за прошедшее время.

Последствия могут быть выражены с помощью денежных, технических персональных критериев влияния или других критериев, значимых для организации. В отдельных случаях для определения последствий, различающихся по времени, месту, группам или ситуациям, требуется более одного цифрового значения.

Последствия, различающиеся по времени или финансам, должны измеряться с использованием того же подхода, который применяется в отношении вероятности угрозы и уязвимости. Должна поддерживаться последовательность количественного или качественного подхода.

Выходные данные. Перечень оцененных последствий сценария инцидентов, выраженных с учетом активов и критериев влияния.

USED AT:	AUTHOR: Бечарев М.И.	DATE: 09.06.2014		WORKING	READER:	DATE:	CONTEXT:
	PROJECT: Оценка риска информационной безопасности	REV: 16.06.2014		DRAFT			TOP
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10			PUBLICATION			



NODE:	TITLE:	NUMBER:
1	Оценка последствий нарушения ИБ, таких, как потеря конфиденциальности, целостности или доступности активов	9

Таблица 3.6

Количественная оценка последствий сценария инцидентов по шкале от 0 до 4

Перечень сценариев инцидентов	Оценка последствий сценария инцидентов
Инцидент с аппаратными средствами	4
Инцидент с программными средствами	4
Инцидент с сетью	3
Инцидент с персоналом	2
Инцидент с местом функционирования организации	1
Инцидент с организацией	3

3.4.3 Оценка вероятности инцидента

Входные данные. Перечень определенных значимых сценариев инцидентов, включая определение угроз, затрагиваемые активы, используемые уязвимости и последствия для активов и бизнес-процессов. Кроме того, перечни всех существующих и планируемых мер и средств контроля и управления, уровень их эффективности, реализации и использования.

Действие. Должна быть оценена вероятность действия сценариев инцидентов.

Руководство по реализации. После определения сценариев инцидентов необходимо оценить вероятность действия каждого сценария и его влияние с использованием качественного или количественного метода установления значения. Необходимо принимать во внимание частоту возникновения угроз и простоту использования уязвимости, с учетом:

- для источников умышленных угроз - мотивации и возможности, которые будут меняться с течением времени, ресурсов, доступных для потенциальных нарушителей, а также восприятия потенциальным нарушителем привлекательности и уязвимости активов;

- опыта и соответствующей статистики вероятности возникновения угроз;
- для источников случайных угроз - территориальных факторов, например близость к химическому или нефтеперерабатывающему заводу, возможность экстремальных погодных условий и факторов, которые могут вызывать ошибки персонала и сбои оборудования;
- существующих мер и средств контроля и управления и того, насколько эффективно они снижают уязвимости;
- уязвимостей как отдельных, так и в совокупности.

В зависимости от требуемой точности активы могут быть сгруппированы или разбиты на элементы, может возникать необходимость соотнесения сценариев с элементами. Так, в зависимости от местоположения характер угроз в отношении одних и тех же видов активов может меняться или различаться эффективность существующих мер и средств контроля и управления.

Выходные данные. Вероятность действия сценариев инцидентов (в количественном или качественном выражении).

USED AT:	AUTHOR: Бочаров М.И.	DATE: 09.06.2014	WORKING	READER	DATE	CONTEXT:
	PROJECT: Оценка риска информационной безопасности	REV: 16.06.2014	DRAFT			TOP
			RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		PUBLICATION			

NODE:	TITLE:	NUMBER:
1	Оценка вероятности инцидента ИБ	10

Таблица 3.7

Оценка вероятности действий сценариев инцидентов по шкале от 0 до 4

Перечень сценариев инцидентов	Оценка последствий сценария инцидентов	Вероятность действия сценариев инцидентов
Инцидент с аппаратными средствами	4	1
Инцидент с программными средствами	4	2
Инцидент с сетью	3	3
Инцидент с персоналом	2	4
Инцидент с местом функционирования организации	1	0
Инцидент с организацией	3	3

3.4.4 Установление значений уровня рисков

Входные данные. Перечень сценариев инцидентов с их последствиями, касающимися активов и бизнес-процессов, и их вероятность (в количественном или качественном выражении).

Действие. Должны быть установлены значения уровня рисков для всех значимых сценариев инцидентов.

Руководство по реализации. При установлении значений рисков присваиваются значения вероятности возникновения риска и его последствий. Эти значения могут быть выражены качественно или количественно. Установление значений рисков основывается на оцененных последствиях и их вероятности. Кроме того, оно может также учитывать стоимость и эффективность, проблемы причастных сторон и другие переменные, используемые при оценке риска. Установленное значение риска является комбинацией значений вероятности сценария инцидента и его последствий.

Выходные данные. Перечень рисков с уровнями присвоенных значений.

Высокоуровневая оценка риска информационной безопасности

Высокоуровневая оценка дает возможность определять приоритеты и хронологию действий. По разным причинам, например, бюджетным, одновременная реализация всех мер и средств контроля и управления не всегда возможна, и с помощью процесса обработки риска могут рассматриваться только наиболее критичные риски. Также может быть преждевременным начинать детальный менеджмент риска, если реализация предусматривается только через год или два. Для достижения этой цели высокоуровневая оценка может начаться с высокоуровневой оценки последствий, а не с систематического анализа угроз, уязвимостей, активов и последствий.

Причиной начать с высокоуровневой оценки является синхронизация с другими планами, связанными с управлением изменениями (или обеспечением непрерывности бизнеса). Например, не имеет смысла обеспечивать полную защиту системы или приложения, если в ближайшем будущем планируется привлечь для работы с ними внешние ресурсы, хотя, возможно, стоит выполнить оценку риска, чтобы определить целесообразность заключения договора о привлечении внешних ресурсов.

При использовании высокоуровневой оценки риска рассматривается ценность для бизнеса информационных активов и риски с точки зрения бизнеса организации. В первой точке принятия решения несколько факторов помогают в определении того, является ли высокоуровневая оценка адекватной для обработки риска; этими факторами могут быть:

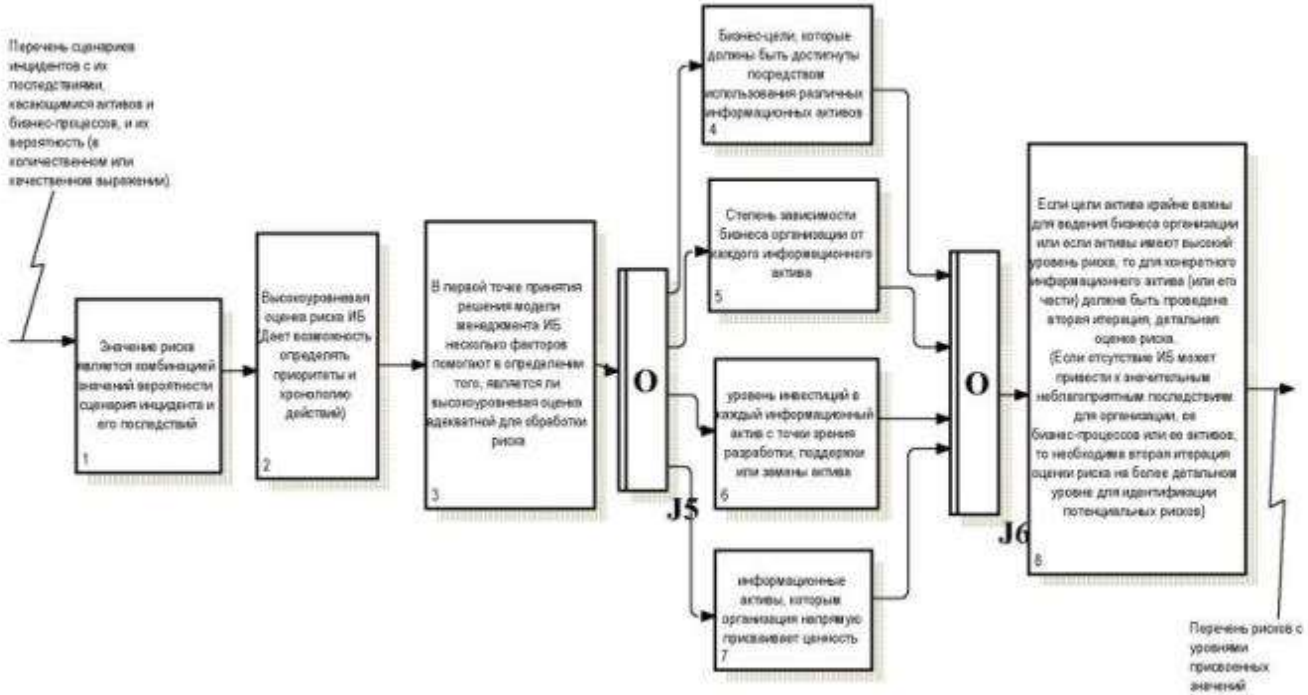
- степень зависимости бизнеса организации от каждого информационного актива (т.е., являются ли функции, которые организация считает критичными для своего выживания или эффективного ведения бизнеса, зависящими от каждого актива или от конфиденциальности, целостности, доступности, неотказуемости, учетности, подлинности и надежности информации, хранящейся и обрабатываемой в данном активе);
- бизнес-цели, которые должны быть достигнуты посредством использования различных информационных активов;

- информационные активы, которым организация напрямую присваивает ценность;
- уровень инвестиций в каждый информационный актив с точки зрения разработки, поддержки или замены актива.

Если цели актива крайне важны для ведения бизнеса организации или если активы имеют высокий уровень риска, то для конкретного информационного актива (или его части) должна быть проведена вторая итерация, детальная оценка риска.

Здесь применяется следующее общее правило: если отсутствие ИБ может привести к значительным неблагоприятным последствиям для организации, ее бизнес-процессов или ее активов, то необходима вторая итерация оценки риска на более детальном уровне для идентификации потенциальных рисков.

USED AT:	AUTHOR: Бочаров М.И.	DATE: 09.06.2014	WORKING	READER	DATE	CONTEXT:
	PROJECT: Оценка риска информационной безопасности	REV: 16.06.2014	DRAFT			TOP
			RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		PUBLICATION			



NODE:	TITLE:	NUMBER:
1	Установление значений уровня рисков ИБ (Высокоуровневая оценка риска ИБ)	11

Детальная оценка риска информационной безопасности

Детальный процесс оценки риска ИБ включает тщательное определение и установление ценности активов, оценку угроз этим активам и оценку уязвимостей. Результаты этой деятельности используются для оценки рисков, а затем для определения способа обработки риска.

Детальная последовательность действий обычно требует продолжительного времени, значительных усилий и компетентности и поэтому может быть наиболее пригодной для информационных систем с высоким уровнем риска.

Окончательным этапом детальной оценки риска ИБ является оценка общих рисков, находящаяся в фокусе данного приложения.

Последствия могут оцениваться несколькими методами, включая количественные, например денежные, и качественные меры (с использованием таких определений, как «умеренные» или «серьезные») или их комбинации. Для оценки вероятности возникновения угрозы должны быть установлены временные рамки, в которых актив будет обладать ценностью или нуждаться в защите.

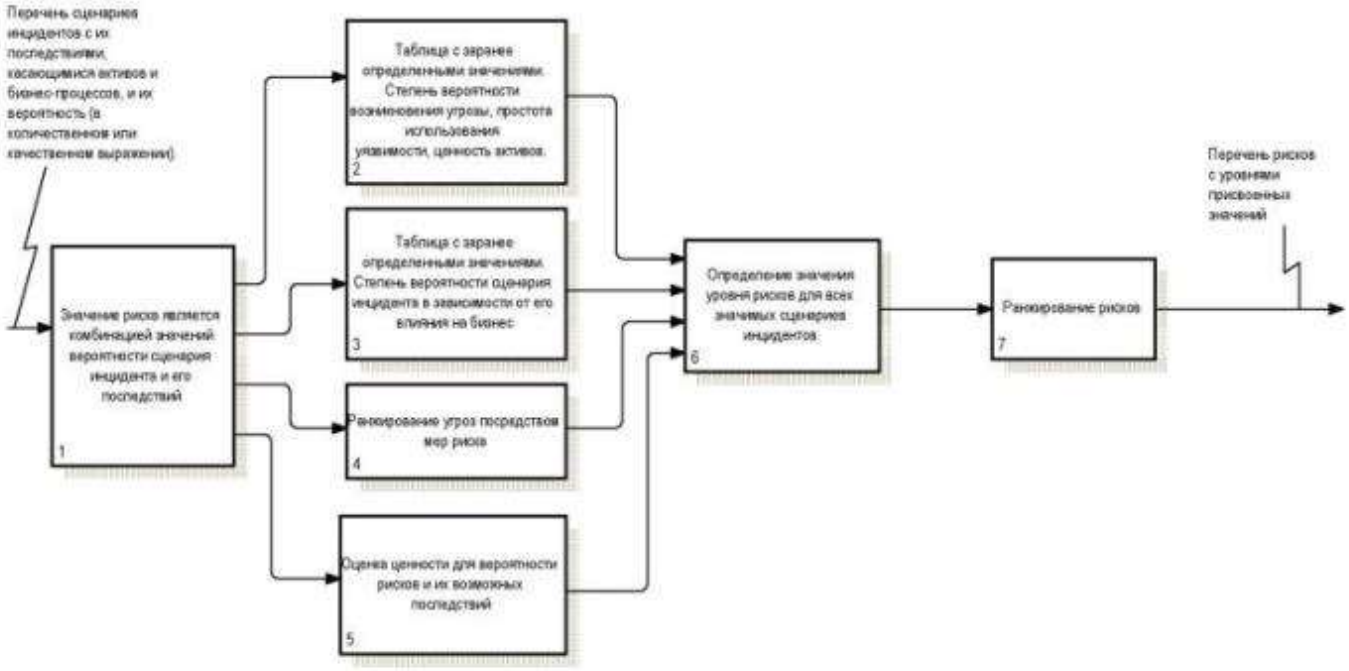
На вероятность возникновения конкретной угрозы оказывают влияние следующие факторы:

- простота преобразования актива, использующего уязвимость за вознаграждение, - применимо при рассмотрении умышленной угрозы со стороны персонала;
- привлекательность актива или возможное воздействие - применимо при рассмотрении умышленной угрозы со стороны персонала;
- чувствительность уязвимости к использованию - применимо к техническим и нетехническим уязвимостям;
- технические возможности действующего фактора угрозы - применимо при рассмотрении умышленной угрозы со стороны персонала.

Во многих методах используются таблицы и объединяются субъективные и эмпирические меры. Важно, чтобы организация

использовала метод, который является для нее наиболее удобным, в котором организация уверена и который будет обеспечивать повторяемость результатов.

USED AT:	AUTHOR: Бочаров М.И.	DATE: 09.06.2014	WORKING	READER:	DATE:	CONTEXT:
	PROJECT: Оценка риска информационной безопасности	REV: 20.06.2014	DRAFT			TOP
	NOTES: 1 2 3 4 5 6 7 8 9 10		RECOMMENDED			
			PUBLICATION			



NODE:	TITLE:	NUMBER:
1	Установление значений уровня рисков ИБ (Детальная оценка риска информационной безопасности)	12

1) **Таблица с заранее определенными значениями**

В методах оценки риска данного вида фактические или предполагаемые физические активы оцениваются с точки зрения стоимости замены или восстановления (т.е. количественные меры). Эта стоимость затем переводится в ту же качественную шкалу, которая используется для информации (см. ниже). Фактические или предполагаемые программные активы оцениваются таким же образом, как и физические активы, - определяется стоимость приобретения или восстановления, а затем переводится в ту же качественную шкалу, которая используется для информации. Кроме того, если считается, что любая прикладная программа имеет собственные присущие ей требования в отношении конфиденциальности или целостности (например, если исходный текст программы сам по себе является коммерчески критичным), она оценивается таким же образом, как и информация.

Ценность информации определяется из опросов отдельных представителей бизнес-менеджмента (владельцев информации), которые могут авторитетно судить о данных с целью определения ценности и критичности фактически используемых данных или данных, которые должны храниться, обрабатываться или оцениваться. Опросы облегчают оценку значимости и критичности информации с точки зрения сценариев наихудших вариантов, возникновение которых можно предполагать исходя из неблагоприятных последствий для бизнеса, обусловленных несанкционированным раскрытием, несанкционированной модификацией, недоступностью в течение различных периодов времени и разрушением.

Ценность определяется использованием принципов определения ценности информации, которые охватывают следующие проблемы:

- личная безопасность;
- юридические и нормативные обязательства;
- личная информация;
- соблюдение законов;

- финансовые потери/нарушение деятельности;
- коммерческие и экономические интересы;
- общественный порядок;
- потеря «неосязаемого капитала»;
- политика и операции бизнеса;
- договор или соглашение с клиентом.

Принципы облегчают определение значений ценности по числовой шкале от 0 до 4, осуществляя таким образом присвоение количественных значений, если это возможно и обоснованно, и качественных значений там, где количественные значения невозможны, например в случае создания опасности для человеческой жизни.

Следующим важным этапом деятельности является заполнение ряда опросных листов для каждого вида угрозы, каждой группы активов, с которой связан данный вид угрозы, чтобы сделать возможной оценку уровней угроз (вероятности возникновения) и уровней уязвимостей (простоты использования угроз для создания неблагоприятных последствий). Каждый ответ на вопрос дает баллы. Эти баллы складываются с использованием базы знаний и сравниваются с диапазонами. Это идентифицирует уровни угроз, например, по шкале от высокого до низкого и, аналогично, уровни уязвимостей (таблица 3.8), с проведением различий между видами последствий. Информация для заполнения опросных листов должна собираться из опросов технического персонала, представителей отдела кадров, из данных обследований фактического месторасположения и проверки документации.

Ценность активов, уровни угроз и уязвимостей, относящиеся к каждому виду последствий, приводятся в табличной форме (матрице), чтобы для каждой комбинации идентифицировать соответствующую меру риска на основе шкалы от 0 до 8. Значения заносятся в матрицу структурированным образом.

Таблица 3.8

Ценность активов, вероятности возникновения угроз, уровни уязвимости

Степень вероятности возникновения угрозы		Низкая			Средняя			Высокая		
Простота использования (уровень уязвимости)		Н	С	В	Н	С	В	Н	С	В
Ценность активов	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Для каждого актива рассматриваются уместные уязвимости и соответствующие им угрозы. Если существует уязвимость без соответствующей угрозы или угроза без соответствующей уязвимости, то в настоящее время риск отсутствует (но следует принимать меры в случае изменения этой ситуации). Соответствующая строка в таблице 3.8 устанавливается по значению ценности актива, а соответствующая колонка устанавливается по степени вероятности возникновения угрозы и простоте использования. Например, если актив имеет ценность 3, угроза является «высокой», а уязвимость «низкой», то мера риска будет равна 5. Предположим, что актив имеет ценность 2 и, например, для модификации уровень угрозы является «низким», а простота использования «высокой», тогда мера риска будет равна 4. Размер таблицы с точки зрения числа категорий вероятности угроз, категорий простоты использования и числа категорий определения ценности активов может быть адаптирован к потребностям организации. Для дополнительных мер риска потребуются дополнительные колонки и строки. Ценность данного подхода заключается в ранжировании рисков, требующих рассмотрения.

Таблица 3.9

Степень вероятности возникновения угрозы			Низкая			Средняя			Высокая		
Простота использования (уровень уязвимости)			Н	С	В	Н	С	В	Н	С	В
Ценность актива	Процесс Процесс поступления-приема на дистанционную форму обучения. Процесс формирования образовательного контента. Процесс получения обучающимся образовательных материалов. Процесс дистанционного оказания обучающемуся консультационных услуг. Процесс отчетности обучающегося и оценка работы обучающегося. Процесс перевода обучающегося на следующий образовательный этап. Процессы маркетинга и обслуживания сайта образовательной организации и системы дистанционного обучения.	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Таблица 3.10

Степень вероятности возникновения угрозы			Низкая			Средняя			Высокая		
Простота использования (уровень уязвимости)			Н	С	В	Н	С	В	Н	С	В
Ценность актива	Информация Информация о персональных данных учащихся и персонала системы дистанционного обучения. Информация о финансовом состоянии организации, предоставляющей услугу дистанционного получения образования. Информационные ресурсы базы данных образовательных электронных курсов	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Таблица 3.11

Степень вероятности возникновения угрозы			Низкая			Средняя			Высокая		
Простота использования (уровень уязвимости)			Н	С	В	Н	С	В	Н	С	В
Ценность актива	Аппаратные средства Серверы, персональные электронные устройства с доступом в сеть Интернет.	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6

Степень вероятности возникновения угрозы			Низкая			Средняя			Высокая		
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Таблица 3.12

Степень вероятности возникновения угрозы			Низкая			Средняя			Высокая		
Простота использования (уровень уязвимости)			Н	С	В	Н	С	В	Н	С	В
Ценность актива	Программные средства Операционная система. Антивирусные средства. Программная среда для организации дистанционного обучения на основе Moodle. Браузеры и плагины к ним для доступа к среде дистанционного обучения.	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Таблица 3.13

Степень вероятности возникновения угрозы			Низкая			Средняя			Высокая		
Простота использования (уровень уязвимости)			Н	С	В	Н	С	В	Н	С	В
Ценность актива	Сеть Телекоммуникационные устройства, используемые для соединения нескольких физически удаленных компьютеров или элементов информационной системы. Устройства, являющиеся не оконечными, а промежуточными устройствами связи. Ретрансляторы, мосты, маршрутизаторы, коммутаторы, концентраторы. Сетевое программное обеспечение управления и мониторинга активного сетевого оборудования. Генерация журналов регистрации.	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Таблица 3.14

Степень вероятности возникновения угрозы			Низкая			Средняя			Высокая		
Простота использования (уровень уязвимости)			Н	С	В	Н	С	В	Н	С	В
Ценность актива	Персонал Администрация организации осуществляющей дистанционную образовательную деятельность. Профессорско-преподавательский состав.	0	0	1	2	1	2	3	2	3	4
		1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7

Степень вероятности возникновения угрозы			Низкая			Средняя			Высокая		
	Менеджеры дистанционного образовательного процесса, специалисты учебной части, методисты, разработчики образовательного контента и контента сайта образовательной организации. Руководитель отдела кадров, руководитель финансового отдела, руководитель, осуществляющий менеджмент риска. Персонал по эксплуатации и сопровождению информационной системы. Разработчики программных элементов среды дистанционного обучения и сайта образовательной организации.	4	4	5	6	5	6	7	6	7	8

Таблица 3.15

Степень вероятности возникновения угрозы			Низкая			Средняя			Высокая		
Простота использования (уровень уязвимости)			Н	С	В	Н	С	В	Н	С	В
Ценность актива	Место функционирования организации	0	0	1	2	1	2	3	2	3	4
	Офис и серверная.	1	1	2	3	2	3	4	3	4	5
	Внешний хостинг сайта.	2	2	3	4	3	4	5	4	5	6
	Удаленные точки доступа к системе дистанционного обучения.	3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Таблица 3.16

Степень вероятности возникновения угрозы			Низкая			Средняя			Высокая		
Простота использования (уровень уязвимости)			Н	С	В	Н	С	В	Н	С	В
Ценность актива	Организация	0	0	1	2	1	2	3	2	3	4
	Организация оказывающая образовательные услуги. Структура организации: Администрация. Кафедры. Организационно-методический отдел. Отдел маркетинга. IT-отдел. Бухгалтерия.	1	1	2	3	2	3	4	3	4	5
		2	2	3	4	3	4	5	4	5	6
		3	3	4	5	4	5	6	5	6	7
		4	4	5	6	5	6	7	6	7	8

Степени вероятности сценария инцидента, отображенного на количественно оцененное влияние бизнеса

Вероятность сценария инцидента дана посредством угрозы, использующей уязвимость с определенной вероятностью. Таблица 3.17 отображает эту вероятность влияния на бизнес, связанную со сценарием инцидента.

Получаемый в результате риск измеряется по шкале от 0 до 8, может быть оценен относительно критериев принятия риска. Данная шкала рисков может также отображаться на простой общий рейтинг рисков, например следующим образом:

- низкий риск: 0 - 2;
- средний риск: 3 - 5;
- высокий риск: 6 - 8.

Таблица 3.17

Степень вероятности сценария инцидента в зависимости от его влияния на бизнес

	Степень вероятности сценария	Очень низкая (очень маловероятна	Низкая (маловероятная)	Средняя (возможная)	Высокая (вероятная)	Очень высокая (частая)
Влияние на бизнес	Очень низкое	0	1	2	3	4
	Низкое	1	2	3	4	5
	Среднее	2	3	4	5	6
	Высокое	3	4	5	6	7
	Очень высокое	4	5	6	7	8

Таблица 3.18

Степень вероятности сценария инцидента в зависимости от его влияния на бизнес в системе дистанционного обучения

Перечень сценариев инцидентов	Степень вероятности сценария инцидента	Влияние на бизнес	Степень вероятности сценария инцидента в зависимости от его влияния на бизнес	Простой общий рейтинг рисков
Инцидент с аппаратными средствами	Низкая	Очень высокое	5	средний риск
Инцидент с программными средствами	Средняя	Высокое	5	средний риск
Инцидент с сетью	Высокая	Высокое	6	высокий риск
Инцидент с персоналом	Очень высокая	Среднее	6	высокий риск
Инцидент с местом функционирования организации	Очень низкая	Очень низкое	0	низкий риск
Инцидент с организацией	Средняя	Низкое	3	средний риск

1) Ранжирование угроз посредством мер риска

Для связи факторов последствий (ценность активов) с вероятностью возникновения угрозы (принимая в расчет аспекты уязвимости) используют таблицу 3.19. В которой перечисляются угрозы (столбец a), над которыми выполняются следующие шаги:

- Первый шаг состоит в оценке последствий (ценности активов) по заранее определенной шкале (определим значения шкалы от 1 до 5), для каждого находящегося под угрозой актива (столбец «b»).
- Второй шаг состоит в оценке степени вероятности возникновения угрозы по заранее определенной шкале, например от 1 до 5, для каждой угрозы (столбец «c»).
- Третий шаг состоит в вычислении меры риска (столбец d) путем умножения (b*c).

- Четвертый шаг ранжируем (столбец e) угрозы в порядке соответствующей меры риска. Отметим, что «1» соответствует наименьшим последствиям и самой низкой степени вероятности возникновения.

Эта процедура, позволяет сопоставить и ранжировать в порядке назначенных приоритетов различные угрозы с разными последствиями и вероятностью возникновения. (В некоторых случаях необходимо результаты, полученные по эмпирическим шкалам, представлять в денежном выражении.)

Таблица 3.19

Ранжирование угроз посредством мер риска

Идентификатор угрозы (a)	Последствия (ценность актива) (b)	Степень вероятности возникновения угрозы (c)	Мера риска (d)	Ранжирование угроз (e)
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Ранее выделенные угрозы ИБ (таблица 3.20)

Таблица 3.20

Группы угроз	Угроза
С аппаратными средствами	Нарушение ремонтопригодности информационных систем
	Ухудшение состояния носителей данных
	Образование пыли, коррозия, замерзание
	Электромагнитное излучение
	Ошибка в использовании
	Потеря электропитания
	Метеорологические явления
	Хищение носителей данных или документов
С программными средствами	Злоупотребление правами
	Порча данных

Группы угроз	Угроза
	Ошибка в использовании
	Фальсификация прав
	Нелегальная обработка данных
	Сбой программных средств
	Тайные действия с программными средствами
	Хищение носителей данных или документов
	Неавторизованное использование оборудования
С сетью	Отказ в осуществлении действий
	Перехват информации
	Отказ телекоммуникационного оборудования
	Фальсификация прав
	Дистанционный шпионаж
	Насыщение информационной системы
	Неавторизованное использование оборудования
С персоналом	Нарушение работоспособности персонала
	Разрушение оборудования или носителей данных
	Ошибка в использовании
	Нелегальная обработка данных
	Хищение носителей данных или документов
	Неавторизованное использование оборудования
С местом функционирования организации	Ухудшение состояния носителей данных
	Затопление
	Отсутствие электропитания
	Хищение аппаратуры
С организацией	Злоупотребление правами
	Нарушение обслуживания информационной системы
	Порча данных
	Данные из ненадежных источников
	Отказ в осуществлении деятельности
	Отказ оборудования
	Ошибка в использовании
	Нелегальная обработка данных
	Хищение оборудования
	Хищение носителей информации или документов
	Неавторизованное использование оборудования
	Использование контрафактных или копированных программных средств

Таблица 3.21

Перечень групп угроз	Степень	Влияние на бизнес

	вероятности угрозы	(ценность актива)
С аппаратными средствами	2 - Низкая	5 - Очень высокое
С программными средствами	3 - Средняя	4 - Высокое
С сетью	4 - Высокая	4 - Высокое
С персоналом	5 - Очень высокая	3 - Среднее
С местом функционирования организации	1 - Очень низкая	1 - Очень низкое
С организацией	3 - Средняя	2 - Низкое

Таблица 3.22

Идентификатор угрозы (a)	Последствия (ценность актива) (b)	Степень вероятности возникновения угрозы (c)	Мера риска (d)	Ранжирование угроз в порядке уменьшения степени риска от 1(максимальный риск) до 6(минимальный риск) (e)
Угроза аппаратным средствам	5	2	10	4
Угроза программным средствам	4	3	12	3
Угроза сети	4	4	16	1
Угроза персоналу	3	5	15	2
Угроза месту функционирования организации	1	1	1	6
Угроза организации	2	3	6	5

3)- Оценка ценности для вероятности рисков и их возможных последствий

В этом примере особое внимание уделяется последствиям инцидентов ИБ (сценариям инцидентов) и определению того, каким системам следует отдавать предпочтение. Это выполняется путем оценки двух значений - для каждого актива и риска, комбинация которых будет определять баллы для каждого актива. Когда суммируются все баллы активов системы, определяется мера риска для этой системы.

Сначала каждому активу присваивается ценность. Это значение связано с возможными неблагоприятными последствиями, которые могут

возникать, если актив находится под угрозой. Эта ценность присваивается активу для каждого случая возникновения соответствующей активу угрозы. Потом оценивается значение вероятности. Оно оценивается исходя из комбинации степени вероятности возникновения угрозы и простоты использования уязвимости (см. таблицу 3.23, выражающую вероятность осуществления сценария инцидентов).

Таблица 3.23

Оценка ценности для степени вероятности и возможных последствий рисков

Уровни угрозы	Низкая			Средняя			Высокая		
Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Значение степени вероятности	0	1	2	1	2	3	2	3	4

Затем, находя пересечение линий значения ценности актива и значения степени вероятности в таблице 3.24, присваиваются баллы активу/угрозе. Баллы актива/угрозы подсчитываются, чтобы получить итоговые баллы для актива. Эта цифра может использоваться для проведения различий между активами, составляющими часть системы.

Таблица 3.24

Ценности актива и значения степени вероятности

Значение степени вероятности	Ценность актива				
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Окончательный шаг заключается в подсчете всех итоговых баллов активов системы, чтобы получить баллы системы. Эта цифра может использоваться для проведения различий между системами и определения того, защите какой системы следует отдавать предпочтение.

Пример.

Предположим, что система С имеет три актива: А1, А2 и А3. Также предположим, что существуют две угрозы У1 и У2, применимые к системе С. Пусть ценность актива А1 будет 3, допустим также, что ценность актива А2 равна 2, а ценность актива А3 равна 4.

Если для А1 и У1 степень вероятности угрозы низкая, а простота использования уязвимости средняя, то значение степени вероятности равно 1 (см. таблицу 3.23).

Баллы для актива/угрозы А1/У1 могут быть выведены из таблицы 3.24 на пересечении линий ценности актива 3 и значения степени вероятности 1, т.е. равные 4. Аналогичным образом, пусть для А1/У2 степень вероятности угрозы будет средней, а простота использования уязвимости будет высокой, что даст для А1/У2 значение 6.

Теперь могут быть вычислены итоговые баллы актива А1У, т.е. равные 10. Итоговые баллы актива вычисляются для каждого актива и применимой угрозы. Итоговые баллы системы вычисляются путем суммирования А1У + А2У + А3У, что дает СУ.

Различные системы могут сравниваться для установления приоритетов, а также различных активов в пределах одной системы.

Активы системы С	Ценность активов
А1	3
А2	2
А3	4

Угрозы системы С соответствующие активу А1
У1
У2

Оценка ценности для степени вероятности и возможных последствий рисков для А1/У1

Уровни угрозы	Низкая			Средняя			Высокая		
Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Значение степени вероятности	0	1	2	1	2	3	2	3	4

Ценности актива и значения степени вероятности для А1/У1

Значение степени вероятности	Ценность актива А1				
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Таким образом, А1У1=4

Для А1/У2

Уровни угрозы	Низкая			Средняя			Высокая		
Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Значение степени вероятности	0	1	2	1	2	3	2	3	4

Для А1/У2

Значение степени вероятности	Ценность актива А1				
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Таким образом, А1/У2 = 6.

Итоговые баллы актива А1 определяются следующей суммой А1У = А1У1+ А1У2=10

Мера риска для всей системы (подсистемы) - СУ будет вычисляться следующим образом СУ=А1У + А2У + А3У.

Приведенные расчеты применимы как к информационным системам, так и к бизнес-процессам.

Итак рассмотрим о**ценку ценности для вероятности рисков и их возможных последствий, применительно к системе дистанционного обучения.**

Из таблицы перечня сценария инцидентов выберем два поля активы и соответствующие им угрозы (таблица 3.25):

Таблица 3.25

Активы и бизнес процессы	Угрозы соответствующие активу
Аппаратные средства: (Актив А1) Серверы. Персональные электронные устройства с доступом в сеть Интернет.	Нарушение ремонтопригодности информационных систем (Угроза У1-1)
	Ухудшение состояния носителей данных (Угроза У1-2)
	Образование пыли, коррозия, замерзание (Угроза У1-3)
	Электромагнитное излучение (Угроза У1-4)
	Ошибка в использовании (Угроза У1-5)
	Потеря электропитания (Угроза У1-6)
	Метеорологические явления (Угроза У1-7)
	Хищение носителей данных или документов (Угроза У1-8)
Программные средства: (Актив А2) Операционная система. Антивирусные средства. Программная среда для организации дистанционного обучения на основе Moodle. Браузеры и плагины к ним для доступа к среде дистанционного обучения.	Злоупотребление правами (Угроза У2-1)
	Порча данных (Угроза У2-2)
	Ошибка в использовании (Угроза У2-3)
	Фальсификация прав (Угроза У2-4)
	Нелегальная обработка данных (Угроза У2-5)
	Сбой программных средств (Угроза У2-6)
	Тайные действия с программными средствами (Угроза У2-7)
	Хищение носителей данных или документов (Угроза У2-8)
	Неавторизованное использование оборудования (Угроза У2-9)
Сеть: (Актив А3) Телекоммуникационные устройства, используемые для соединения нескольких физически удаленных компьютеров или элементов информационной системы. Устройства, являющиеся не оконечными, а	Отказ в осуществлении действий (Угроза У3-1)
	Перехват информации (Угроза У3-2)
	Отказ телекоммуникационного оборудования (Угроза У3-3)
	Фальсификация прав (Угроза У3-4)
	Дистанционный шпионаж (Угроза У3-5)
	Насыщение информационной системы (Угроза У3-6)

Активы и бизнес процессы	Угрозы соответствующие активу
промежуточными устройствами связи. Ретрансляторы, мосты, маршрутизаторы, коммутаторы, концентраторы. Сетевое программное обеспечение управления и мониторинга активного сетевого оборудования. Генерация журналов регистрации.	Неавторизованное использование оборудования (Угроза У3-7)
Персонал: (Актив А4) Администрация организации осуществляющей дистанционную образовательную деятельность. Профессорско-преподавательский состав. Менеджеры дистанционного образовательного процесса, специалисты учебной части, методисты, разработчики образовательного контента и контента сайта образовательной организации. Руководитель отдела кадров, руководитель финансового отдела, руководитель, осуществляющий менеджмент риска. Персонал по эксплуатации и сопровождению информационной системы. Разработчики программных элементов среды дистанционного обучения и сайта образовательной организации.	Нарушение работоспособности персонала (Угроза У4-1)
	Разрушение оборудования или носителей данных (Угроза У4-2)
	Ошибка в использовании (Угроза У4-3)
	Нелегальная обработка данных (Угроза У4-4)
	Хищение носителей данных или документов (Угроза У4-5)
	Неавторизованное использование оборудования (Угроза У4-6)
Место функционирования организации: (Актив А5) Офис и серверная. Внешний хостинг сайта. Удаленные точки доступа к системе дистанционного обучения.	Ухудшение состояния носителей данных (Угроза У5-1)
	Затопление (Угроза У5-2)
	Отсутствие электропитания (Угроза У5-3)
	Хищение аппаратуры (Угроза У5-4)
Организация: (Актив А6) Организация оказывающая образовательные услуги. Структура организации: Администрация. Кафедры.	Злоупотребление правами (Угроза У6-1)
	Нарушение обслуживания информационной системы (Угроза У6-2)
	Порча данных (Угроза У6-3)
	Данные из ненадежных источников (Угроза У6-4)
	Отказ в осуществлении деятельности (Угроза У6-5)
	Отказ оборудования (Угроза У6-6)

Активы и бизнес процессы	Угрозы соответствующие активу
Организационно-методический отдел. Отдел маркетинга. IT-отдел. Бухгалтерия.	Ошибка в использовании (Угроза У6-7)
	Нелегальная обработка данных (Угроза У6-8)
	Хищение оборудования (Угроза У6-9)
	Хищение носителей информации или документов (Угроза У6-10)
	Неавторизованное использование оборудования (Угроза У6-11)
	Использование контрафактных или копированных программных средств (Угроза У6-12)

Рассчитаем меру риска для каждой группы актива и для всей системы в целом (таблица 3.26).

Таблица 3.26

Актив	Ценность актива
Аппаратные средства	4
Программные средства	3
Сеть	3
Персонал	2
Место функционирования организации	0
Организация	1

1) Аппаратные средства: (Актив группы А1)

(Актив А1)/(Угроза У1-1)=8

(Актив А1)/(Угроза У1-2)=7

(Актив А1)/(Угроза У1-3)=4

(Актив А1)/(Угроза У1-4)=4

(Актив А1)/(Угроза У1-5)=5

(Актив А1)/(Угроза У1-6)=6

(Актив А1)/(Угроза У1-7)=4

(Актив А1)/(Угроза У1-8)=7

(Актив А1)/(Угрозы У1)=(Актив А1)/(Угроза У1-1)+(Актив А1)/(Угроза У1-2)+(Актив А1)/(Угроза У1-3)+(Актив А1)/(Угроза У1-4)+(Актив А1)/(Угроза У1-5)+(Актив А1)/(Угроза У1-6)+(Актив А1)/(Угроза У1-7)+(Актив А1)/(Угроза У1-8)=8+7+4+4+5+6+4+7=**30**

2) Программные средства:

(Актив А2)/(Угроза У2-1)=3

(Актив А2)/(Угроза У2-2)=4

(Актив А2)/(Угроза У2-3)=3

(Актив А2)/(Угроза У2-4)=3

(Актив А2)/(Угроза У2-5)=4

(Актив А2)/(Угроза У2-6)=5

(Актив А2)/(Угроза У2-7)=3

(Актив А2)/(Угроза У2-8)=6

(Актив А2)/(Угроза У2-9)=3

(Актив А2)/(Угрозы У2)= (Актив А2)/(Угроза У2-1)+(Актив А2)/(Угроза У2-2)+(Актив А2)/(Угроза У2-3)+(Актив А2)/(Угроза У2-4)+(Актив А2)/(Угроза У2-5)+(Актив А2)/(Угроза У2-6)+(Актив А2)/(Угроза У2-7)+(Актив А2)/(Угроза У2-8)+(Актив А2)/(Угроза У2-9)=3+5+4+3+4+5+4+6+3=**37**

3) Сеть:

(Актив А3)/(Угроза У3-1)=7

(Актив А3)/(Угроза У3-2)=6

(Актив А3)/(Угроза У3-3)=7

(Актив А3)/(Угроза У3-4)=3

(Актив А3)/(Угроза У3-5)=4

(Актив А3)/(Угроза У3-6)=5

(Актив А3)/(Угроза У3-7)=6

(Актив А3)/(Угрозы У3)= (Актив А3)/(Угроза У3-1)+(Актив А3)/(Угроза У3-2)+(Актив А3)/(Угроза У3-3)+(Актив А3)/(Угроза У3-4)+(Актив А3)/(Угроза У3-5)+(Актив А3)/(Угроза У3-6)+(Актив А3)/(Угроза У3-7)=7+6+7+3+4+5+6=**38**

4) Персонал:

(Актив А4)/(Угроза У4-1)=5

(Актив А4)/(Угроза У4-2)=4

(Актив А4)/(Угроза У4-3)=6

(Актив А4)/(Угроза У4-4)=5

(Актив А4)/(Угроза У4-5)=6

(Актив А4)/(Угроза У4-6)=5

(Актив А4)/(Угрозы У4)= (Актив А4)/(Угроза У4-1)+(Актив А4)/(Угроза У4-2)+(Актив А4)/(Угроза У4-3)+(Актив А4)/(Угроза У4-4)+(Актив А4)/(Угроза У4-5)+(Актив А4)/(Угроза У4-6)=5+4+6+5+6+5=**31**

5) Место функционирования организации:

(Актив А5)/(Угроза У5-1)=3

(Актив А5)/(Угроза У5-2)=0

(Актив А5)/(Угроза У5-3)=4

(Актив А5)/(Угроза У5-4)=2

(Актив А5)/(Угрозы У5)=(Актив А5)/(Угроза У5-1)+(Актив А5)/(Угроза У5-2)+(Актив А5)/(Угроза У5-3)=4+(Актив А5)/(Угроза У5-4)=3+0+4+2=**9**

6) Организация:

(Актив А6)/(Угроза У6-1)=2

(Актив А6)/(Угроза У6-2)=4

(Актив А6)/(Угроза У6-3)=2

(Актив А6)/(Угроза У6-4)=2

(Актив А6)/(Угроза У6-5)=3

(Актив А6)/(Угроза У6-6)=2

(Актив А6)/(Угроза У6-7)=3

(Актив А6)/(Угроза У6-8)=1

(Актив А6)/(Угроза У6-9)=1

(Актив А6)/(Угроза У6-10)=5

(Актив А6)/(Угроза У6-11)=2

(Актив А6)/(Угроза У6-12)=1

(Актив А5)/(Угрозы У5)=(Актив А6)/(Угроза У6-1)+(Актив А6)/(Угроза У6-2)+(Актив А6)/(Угроза У6-3)+(Актив А6)/(Угроза У6-4)+(Актив А6)/(Угроза У6-5)+(Актив А6)/(Угроза У6-6)+(Актив А6)/(Угроза У6-7)+(Актив А6)/(Угроза У6-8)+(Актив А6)/(Угроза У6-9)+(Актив А6)/(Угроза У6-10)+(Актив А6)/(Угроза У6-11)+(Актив А6)/(Угроза У6-12)=2+4+2+2+3+2+3+1+1+5+2+1=28

Таблица 3.27

	Активы	Оценка ценности для вероятности рисков и их возможных последствий	Ранжирование угроз в порядке уменьшения степени риска от 1(максимальный риск) до 5(минимальный риск)
1	Аппаратные средства:	30	4
2	Программные средства	37	2
3	Сеть	38	1
4	Персонал	31	3
5	Место функционирования организации	9	6
6	Организация	28	5

3.5 Оценка риска

Входные данные. Перечень рисков с уровнями присвоенных значений и критериями оценки риска.

Действие. Должны сравниваться уровни рисков с критериями оценки рисков и критериями принятия рисков [связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление е) 4)].

Руководство по реализации. Характер решений, связанных с оценкой рисков, и критерии оценки рисков, которые будут использованы для принятия этих решений, должны определяться при установлении контекста. Эти решения и контекст должны более детально анализироваться на этапе получения большего объема информации о конкретных идентифицированных рисках. Для оценки рисков организация должна сравнивать установленные значения рисков (с использованием выбранных методов, рассматриваемых в приложении) с критериями оценки риска, выбранными на этапе установления контекста.

Критерии оценки риска, используемые для принятия решений, должны согласовываться с определенным внешним и внутренним контекстом менеджмента риска ИБ и учитывать цели организации, мнения причастных

сторон и т.д. Решения, связанные с оценкой риска, обычно основываются на приемлемом уровне риска. Однако также должны учитываться последствия, вероятность, степень уверенности при идентификации и анализе риска. Совокупность множества рисков низкого и среднего уровня в итоге может иметь результатом общий риск более высокого уровня.

При этом необходимо учитывать следующее:

- значимость бизнес-процесса или деятельности, поддерживаемых конкретным активом или совокупностью активов, если процесс определен как имеющий низкую значимость, связанным с ним рискам следует уделять меньше внимания, чем рискам, влияющим на более важные процессы или деятельность;
- свойства ИБ - если один критерий не актуален для организации (например, потеря конфиденциальности), то все риски, влияющие на этот критерий, могут быть также не актуальными.

Оценка риска основывается на понимании риска, полученном при анализе риска, и используется при принятии решений о будущих действиях. Решения должны включать в себя следующее:

- приоритеты при обработке риска с учетом установленных значений уровней рисков;
- необходимость в некой деятельности.

На стадии оценки риска в дополнение к рискам с установленными значениями должны приниматься в расчет договорные, юридические и нормативные требования.

Выходные данные. Перечень рисков с назначенными приоритетами в соответствии с критериями оценки рисков, касающимися сценариев инцидентов, которые приводят к этим рискам.

Заключение

1. Выполнен анализ современных подходов организации систем управления информационными услугами в результате которого определен подход управления ИТ-услугами – IT Service Management (ITSM)в основе которого расположен клиент и его потребности в услугах, предоставляемых с помощью информационных технологий. Причем данный подход сочетает в себе процессную организацию предоставления услуг и зафиксированные в соглашениях об уровне услуг ключевые показатели эффективности (Key Performance Indicators, KPI), что говорит о системности и измеряемости и контролируемости качества предоставления услуги и соответственно управляемости данного процесса. Управление ИТ-услугами реализуется поставщиками ИТ-услуг путем использования наиболее оптимального сочетания людей, процессов и информационных технологий.

2. Выполнен анализ современных подходов организации систем управления информационной безопасностью на основе комплекс документов – IT Infrastructure Library (ITIL)информационно-методической поддержки подхода управления ИТ-услугами разработан. Выявлены особенности нового подхода Service life cycle – «жизненного цикла сервиса» к ITSM, который заключается в предложенной стратегии сервисов: проектирование сервисов, передача сервисов, эксплуатация сервисов и к постоянное улучшение сервисов как наиболее универсального для создания типовых решений управления информационными услугами.

3. Разработано типовое решение управления услугами и оценки риска ИБ в рамках системы менеджмента информационной безопасности на примере системы дистанционного обучения.

4. Разработаны рекомендации по созданию типовых решений организации систем управления информационными услугами и информационной безопасностью для организаций различного профиля

содержащие типовую методику расчета рисков информационной безопасности организации

Список литературы

1. Использование типовых программных компонентов в системах управления предприятиями http://knowledge.allbest.ru/programming/2c0b65625a3ad68a5c43a88521316c36_1.html.
2. Словарь терминов ITIL® на русском языке, версия 1.0, 29 июля 2011 г. на основе английской версии 1.0, 29 июля 2011. Crown Copyright 2011.
3. ITIL & ITSM World / http://www.itil-itsm-world.com.
4. Потоцкий М. Обзор стандарта ISO 20000-1:2011, отличия от версии 2005 года // Information Management, №01, 2011. С. 29-33.
5. Зырянов М. Сервисный подход к информационной безопасности / «Директор информационной службы», № 01, 2013. http://www.osp.ru/cio/2013/01/13033706/.
6. Всеобщее управление качеством: учебник / В.Н. Азаров, В.П. Майборода, А.Ю. Панычев, Ю.А. Усманов – М.: ФГБОУ « Учебно-методический центр по образованию на железнодорожном транспорте», 2013. -572 с.
7. Лукацкий А. Что должен знать ИТ-директор об информационной безопасности в России / «Директор информационной службы», № 05, 2011 http://www.osp.ru/cio/2011/05/13008814/.
8. Кузнецов С. Кибербезопасность в XXI веке / «Открытые системы», № 05, 2013. http://www.osp.ru/os/2013/05/13036002/.
9. Бурносова О. О двух подходах к описанию бизнес-процессов ИТ-подразделений / http://www.iteam.ru/publications/it/section_51/article_2750/.
10. Маркин Д.П. Непрерывность бизнеса стала социальной // "Information Security/ Информационная безопасность" №4, 2012. - С. 52.
11. Кораблев С. Сравнение DLP-систем // «Windows IT Pro», № 01, 2014.

Список дополнительной литературы

1. ИТ-Сервис-менеджмент. Введение. М. 2003.

2. Введение в реальный ITSM / Роб Ингланд; Пер. с англ. – М.: Лайвбук, 2010. – 132 с.
3. Овладевая ITIL / Роб Ингланд; Пер. с англ. – М.: Лайвбук, 2011. – 200 с.
4. Методические рекомендации по формированию требований к обеспечению информационной безопасности информационных систем и ресурсов города Москвы. Классификатор конфиденциальной информации, содержащейся в информационных системах и ресурсах города Москвы. Утверждено Мэром Москвы 29 ноября 2006 года. / http://www.iso27000.ru/zakonodatelstvo/dokumenty-pravitelstva-moskvy-v-oblasti-informacionnoi-bezopasnosti/metodicheskie-rekomendacii-po-formirovaniyu-trebovanii-k-obespecheniyu-informacionnoi-bezopasnosti-informacionnyh-sistem-i-resursov-goroda-moskvy/
5. Информационная безопасность и анализ угроз / http://bezopasnik.org/article/21.htm

ГОСТЫ

1. BS ISO 22301:2012 Социальная безопасность – Система менеджмента непрерывности деятельности – Требования; Новый стандарт в области непрерывности деятельности, пришедший на замену BS 25999-2;
2. BS ISO/IEC 27031:2011 Информационные технологии – Техника обеспечения безопасности – Руководство для информационных и коммуникационных технологий по готовности к непрерывности бизнеса;
3. BS ISO/IEC 27005:2011 Информационные технологии – Техника обеспечения безопасности – Менеджмент рисков информационной безопасности;
4. BS ISO 22313:2012 Социальная безопасность – Система менеджмента непрерывности деятельности – Руководство;
5. BS ISO 31000:2009 Управление рисками – Принципы и руководство.