

Стандарты информационной безопасности

Лекция 5. Системы менеджмента информационной безопасностью. Требования

Направление подготовки (специальность):

090303 Информационная безопасность автоматизированных систем

Руководитель занятий:

Куприянов Александр Олегович

Количество часов:

2 часа

Системы менеджмента информационной безопасностью. Требования

План лекции

1	Процессный подход в менеджменте информационной безопасностью
2	Планирование. Разработка системы менеджмента информационной безопасности
3	Цели и меры управления
4	Документирование политики информационной безопасности (5.1.1 ГОСТ ИСО/МЭК 27002)
5	Требования. Связь целей и мер управления

Терминология

27000
Общий обзор и словарь

Стандарты с требованиями

27001
Системы менеджмента информационной безопасности – Требования

27006
Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности

Стандарты с рекомендациями

27002
Свод правил по управлению защитой информации

ТО 27008
Руководящие указания для аудиторов по оценке органов управления

27003
Руководство по внедрению системы менеджмента информационной безопасности

27013
Руководство по интегрированному внедрению ISO/IEC 27001 и ISO/IEC 20000-1

27004
Менеджмент информационной безопасности - Измерения

27014
Руководство по информационной безопасности

27005
Менеджмент риска информационной безопасности

ТО 27016
Менеджмент информационной безопасности – Организационная экономика

27007
Руководящие указания по аудиту систем менеджмента систем информационной безопасности

27010
Руководящие указания по обеспечению защиты информационного обмена между подразделениями и организациями

ТО 27015
Руководящие указания по менеджменту защиты информации для финансовых операций

Стандарты для специальных областей

27011
Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002

ТС 27017
Свод правил для средств управления информационной безопасностью на основе ISO/IEC 27002 для облачных сервисов

ISO/IEC 27001

Современные практики по управлению СМИБ базируются на международном стандарте ISO/IEC 27001.

Аутентичным аналогом международного стандарта ISO/IEC 27001 является национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27001-2006.

ISO/IEC 27001

<p>ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements</p>	<p>Information techniques. management</p>	<p>А Н Л О Г</p>	<p>ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования</p> <p style="text-align: center;">Аутентичен</p>
			<p>ISO/IEC 27001:2005 Information technology. Security techniques. Information security management systems. Requirements</p>

Процессный подход в менеджменте информационной безопасностью

Любой вид деятельности, использующий ресурсы и управляемый для того, чтобы дать возможность преобразования входов в выходы, можно считать процессом. Часто выход одного процесса непосредственно образует вход следующего процесса.

Особую важность для пользователей при осуществлении процессного подхода применительно к менеджменту информационной безопасности имеют следующие факторы:

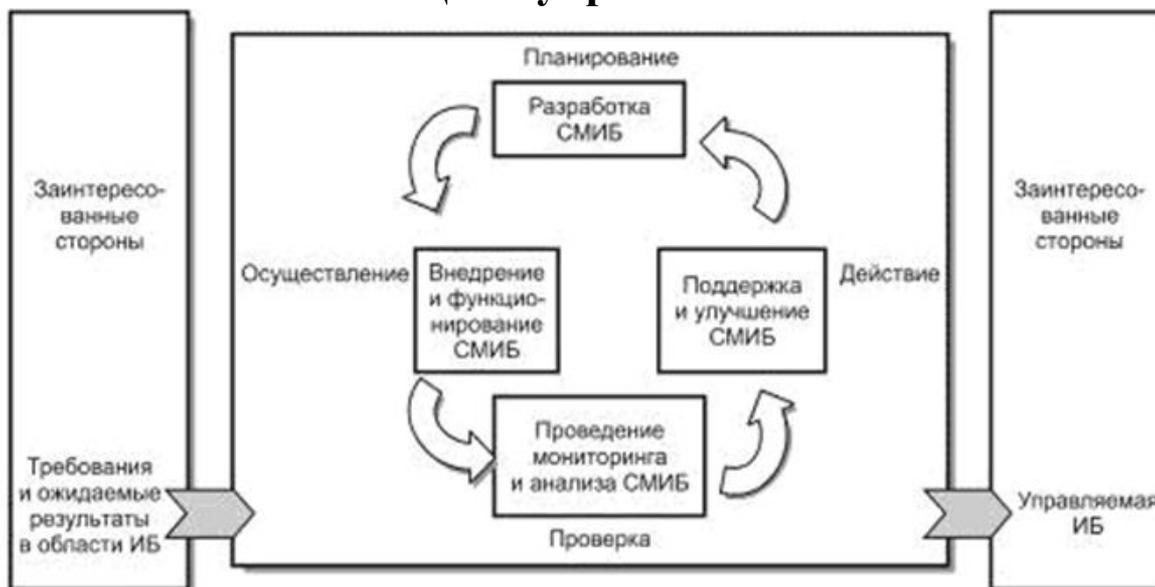
- понимание требований информационной безопасности организации и необходимости установления политики и целей информационной безопасности;
- внедрение и использование мер управления для менеджмента рисков информационной безопасности среди общих бизнес-рисков организации;
- мониторинг и проверка эффективности СМИБ;
- непрерывное улучшение СМИБ, основанное на результатах объективных измерений.

Циклически повторяющийся процесс принятия решения, используемый в управлении качеством называется – цикл Деминга (Цикл PDCA).

PDCA (англ. «*Plan-Do-Check-Act*» - планирование-действие-проверка-корректировка) циклически повторяющийся процесс принятия решения, используемый в управлении качеством.

Процессный подход в менеджменте информационной безопасностью

Цикл управления



Планирование (разработка СМИБ)	Разработка политики, установление целей, процессов и процедур СМИБ, относящихся к менеджменту риска и улучшению информационной безопасности, для достижения результатов, соответствующих общей политике и целям организации
Осуществление (внедрение и обеспечение функционирования СМИБ)	Внедрение и применение политики информационной безопасности, мер управления, процессов и процедур СМИБ
Проверка (проведение мониторинга и анализа СМИБ)	Оценка, в том числе, по возможности, количественная, результативности процессов относительно требований политики, целей безопасности и практического опыта функционирования СМИБ и информирование высшего руководства о результатах для последующего анализа
Действие (поддержка и улучшение СМИБ)	Проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения СМИБ

Процессный подход в менеджменте информационной безопасностью

Планирование	Выполнение	Проверка	Воздействие (управление, корректировка)
установление целей и процессов, необходимых для достижения целей, планирование работ по достижению целей процесса и удовлетворения потребителя, планирование выделения и распределения необходимых ресурсов	выполнение запланированных работ	сбор информации и контроль результата на основе ключевых показателей эффективности (KPI), получившегося в ходе выполнения процесса, выявление и анализ отклонений, установление причин отклонений	принятие мер по устранению причин отклонений от запланированного результата, изменения в планировании и распределении ресурсов

Процессный подход в менеджменте информационной безопасностью

Система менеджмента информационной безопасности; СМИБ (information security management system; ISMS): Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности. Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы.

Процессный подход в менеджменте информационной безопасностью

Основные принципы, которые способствуют успешной реализации СМИБ:

понимание необходимости системы информационной безопасности

назначение ответственности за информационную безопасность

соединение административных обязанностей и интересов заинтересованных лиц

возрастание социальных ценностей

оценка риска, определяющая соответствующие меры и средства контроля и управления для достижения допустимых уровней риска

безопасность как неотъемлемый существенный элемент информационных сетей и систем

активное предупреждение и выявление инцидентов информационной безопасности

обеспечение комплексного подхода к менеджменту информационной безопасности

непрерывная переоценка и соответствующая модификация системы информационной безопасности

Планирование. Разработка системы менеджмента информационной безопасности

Перечень мероприятий по разработке СМИБ:

- определить область применения СМИБ;
- определить политику СМИБ;
- определить подход к оценке риска в организации;
- идентифицировать риски;
- проанализировать и оценить риски;
- определить и оценить различные варианты обработки рисков;
- выбрать цели и меры управления для обработки рисков;
- получить утверждение руководством предполагаемых остаточных рисков;
- получить разрешение руководства на внедрение и эксплуатацию СМИБ;
- подготовить Положение о применимости.

Система менеджмента информационной безопасности. Планирование

Определение области применения СМИБ с учётом характеристик бизнеса, организации, её размещения, активов и технологий, включая детали и обоснование любых исключений из области её действия

Политика СМИБ

Содержит структуру для её целей и даёт общее представление об управлении и принципах действий в сфере информационной безопасности

принимает во внимание требования бизнеса, правовые и инструктивные требования, а также договорные обязательства по безопасности

выстраивает стратегический контекст менеджмента риска организации, в котором будет создаваться и поддерживаться СМИБ

задает критерии, относительно которых будет оцениваться риск

утверждается руководством организации

Оценка риска

Определить методологию оценки риска, подходящую для СМИБ (соответствует требованиям обеспечения деятельности организации и нормативно-правовым требованиям ИБ)

Разработать критерии принятия рисков и установить приемлемый уровень риска

методология оценки риска должна обеспечить сравнимые и воспроизводимые результаты
(ГОСТ Р ИСО/МЭК ТО 13335–3 *Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасностью информационных технологий*)

Идентификация рисков

Идентифицировать активы, относящиеся к области применения СМИБ, и определить собственников этих активов

Идентифицировать угрозы этим активам

идентифицировать уязвимости, которые могут быть использованы этими угрозами

идентифицировать последствия воздействия на активы в результате возможной утраты конфиденциальности, доступности и целостности активов

Анализ и оценка рисков

Оценить ущерб бизнесу, который может быть нанесен в результате нарушения безопасности, с учетом возможных последствий нарушения безопасности

Оценить реальную вероятность возникновения нарушения безопасности с учётом преобладающих угроз и уязвимостей

Оценить уровни рисков

Определить, являются ли риски приемлемыми или требуют обработки с использованием критериев допустимости рисков

Обработка рисков

Применение подходящих мер управления

Сознательное и объективное принятие рисков при условии соответствия требованиям политики и критериям организации в отношении принятия рисков

Избегание рисков

Передача соответствующих деловых рисков сторонним организациям (страховщикам или поставщикам)

Цели и меры управления

Цели и меры управления изложены в приложении А к стандарту ISO/IEC 27001. В стандарте ISO/IEC 27002 предоставляется более детализированная информация для поддержки реализации мер и средств контроля и управления и достижения целей управления. Меры и средства контроля и управления информационной безопасности в стандарте изложены в 11-ти разделах, которые все вместе содержат, в целом, 39 основных категорий безопасности, и одного вводного раздела, знакомящего с оценкой и обработкой рисков.

В международном стандарте ISO/IEC 27003 рассматриваются важнейшие аспекты, необходимые для успешной разработки и внедрения системы менеджмента информационной безопасности (СМИБ) в соответствии со стандартом ISO/IEC 27001:2005. В нем описывается процесс определения и разработки СМИБ от запуска до составления планов внедрения. В нем описывается процесс получения одобрения руководством внедрения СМИБ, определяется проект внедрения СМИБ (упоминается в данном международном стандарте как проект СМИБ) и представлены рекомендации по планированию проекта СМИБ, в результате которого получается окончательный план внедрения СМИБ.

Документирование политики информационной безопасности

(5.1.1 ГОСТ ИСО/МЭК 27002)

Политика информационной безопасности документирует стратегическую позицию организации в отношении информационной безопасности во всей организации.

Политика строится на основе информации и знания. Моменты, признанные руководством важными во время ранее проведенного анализа, должны быть сделаны наглядными, им должно быть уделено особое внимание в политике, чтобы обеспечить стимуляцию и мотивацию в организации. Также важно отметить, что происходит, если не следовать выбранной политике, и подчеркнуть влияния законов и регулирующих положений на рассматриваемую организацию.

Мера и средство контроля и управления.

Политика информационной безопасности должна быть утверждена руководством, издана и доведена до сведения всех сотрудников организации и соответствующих сторонних организаций.

Документирование политики информационной безопасности

(5.1.1 ГОСТ ИСО/МЭК 27002)

Рекомендация по реализации.

Политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к менеджменту информационной безопасности, Документ, в котором излагается политика, должен содержать положения относительно:

- a. определения информационной безопасности, ее общих целей и сферы действия, а также упоминания значения безопасности как инструмента, обеспечивающего возможность совместного использования информации;
- b. изложения намерений руководства, поддерживающих цели и принципы информационной безопасности в соответствии со стратегией и целями бизнеса;
- c. подхода к установлению мер и средств контроля и управления и целей их применения, включая структуру оценки риска и менеджмента риска;
- d. краткого разъяснения наиболее существенных для организации политик безопасности, принципов, стандартов и требований соответствия: например:
 - соответствие законодательным требованиям и договорным обязательствам;
 - требования по обеспечению осведомленности, обучения и тренинга в отношении безопасности;
 - менеджмент непрерывности бизнеса;
 - ответственность за нарушения политики информационной безопасности;
- e. определения общих и конкретных обязанностей сотрудников в рамках менеджмента информационной безопасности, включая информирование об инцидентах безопасности;
- f. ссылок на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Требования. Связь целей и мер управления

В приложение А к стандарту ГОСТ Р ИСО/МЭК 27001-2006 приведена связь целей и мер управления.

В разделах 5-15 ИСО/МЭК 17799:2005 приведены рекомендации по реализации и указания с точки зрения практики в отношении поддержки мер управления, изложенных в А.5-А.15.

ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Свод норм и правил менеджмента информационной безопасности» заменил ГОСТ Р ИСО/МЭК 17799-2005. ГОСТ Р ИСО/МЭК 27002-2012 является аналогом ISO/IEC 27002:2005 «Information technology - Security techniques - Code of practice for information security management».