Московский университет МВД России им. В. Я. Кикотя
Кафедра «Специальных информационных систем»

ГОСТ Р ИСО/МЭК 27001 – 2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

Лекция 3

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Система менеджмента информационной безопасности (СМИБ) – часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Целью построения СМИБ является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов
и гарантирующих доверие заинтересованных сторон.

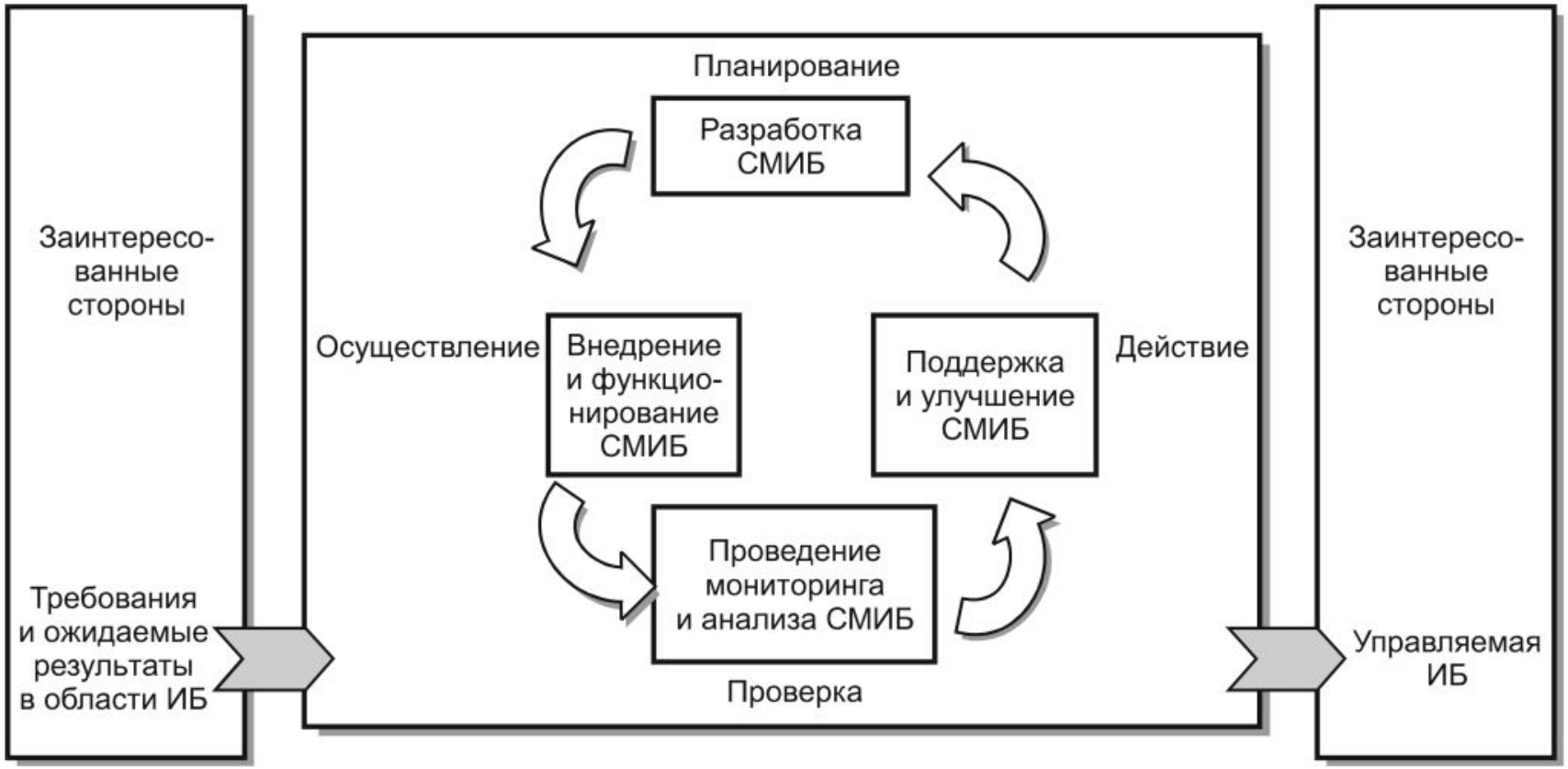
РАЗРАБОТКА СМИБ

Организации необходимо:

a) определить область и границы действия СМИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий, в том числе детали и обоснование любых исключений из области ее действия;
b) определить политику СМИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий;
c) определить подход к оценке риска в организации;
d) идентифицировать риски;
e) проанализировать и оценить риски;
f) определить и оценить различные варианты обработки рисков;
g) выбрать цели и меры управления для обработки рисков.

ПРОЦЕССЫ СМИБ

Модель «Планирование (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (PDCA)



ПРОЦЕССЫ СМИБ

Связи между процессами СМИБ модели PDCA

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

Модель позволяет осуществить оценку рисков, проектирование и реализацию системы информационной безопасности, ее менеджмент и переоценку

ПОЛИТИКА СМИБ

Политика СМИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий должна включать в себя:

a) концепцию, включающую в себя цели, основные направления и принципы действий в сфере ИБ;
b) принятие во внимание требования бизнеса, нормативно-правовые требования, а также договорные обязательства по обеспечению безопасности;
c) согласование со стратегическим содержанием менеджмента рисков организации, в рамках которого будет разрабатываться и поддерживаться СМИБ;
d) установление критериев оценки рисков.

Политика СМИБ утверждается руководством организации.

ДОКУМЕНТАЦИЯ СМИБ

Документация СМИБ должна включать в себя следующее:

a) документированные положения политики СМИБ и целей СМИБ;
b) область функционирования СМИБ;
c) процедуры и меры управления, поддерживающие СМИБ;
d) описание методологии оценки риска;
e) отчет по оценки риска;
f) план обработки рисков;
g) документированные процедуры, необходимые организации для обеспечения эффективного планирования процессов в области ИБ и управления этими процессами, а также описания путей оценки результативности мер управления;
h) учетные записи;
i) положение о применимости.

УПРАВЛЕНИЕ ДОКУМЕНТАМИ

Документированная процедура определяет действия руководства по:

a) утверждению документов СМИБ перед их изданием;

b) пересмотру, обновлению и повторному утверждению документов;

c) обеспечению идентификации внесенных изменений и текущего статуса документов;

d) обеспечению наличия версий соответствующих документов в местах их использования;

e) определению порядка просмотра документов и их идентификации;

f) обеспечению доступа к документам авторизованным лицам, а также передачи, хранения и уничтожения в соответствии с процедурами, применимыми к степени их конфиденциальности;

g) идентификации документов, созданных вне организации;

h) обеспечению контроля за распространением документов;

i) предотвращению непреднамеренного использования устаревших документов;

j) использованию соответствующей идентификации устаревших

УПРАВЛЕНИЕ ЗАПИСЯМИ

Для предоставления свидетельств соответствия требованиям и результативности функционирования СМИБ необходимо вести и поддерживать в рабочем состоянии учетные записи.
Учетные записи необходимо контролировать и защищать. СМИБ должна принимать во внимание все нормативно-правовые требования и договорные обязательства, имеющие отношение к ИБ. Записи должны быть четкими, легко идентифицируемыми и восстанавливаемыми.
Меры управления, требуемые для идентификации, хранения, защиты, поиска, определения сроков хранения и уничтожения записей должны быть документированы и реализованы.

Примерами записей являются: журнал регистрации посетителей, отчеты о результатах аудитов, заполненные формы авторизации доступа.

ЦЕЛИ И МЕРЫ УПРАВЛЕНИЯ

Данный перечень мер управления не является исчерпывающим и организация может рассмотреть необходимость дополнительных целей и мер управления

A.5 Политика безопасности		
A.5.1 Политика информационной безопасности Цель: Обеспечить участие высшего руководства организации в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами		
A.5.1.1	Документирование политики информационной безопасности	Политика информационной безопасности должна быть руководством утверждена, издана и доведена до сведения всех сотрудников организации, а также сторонних организаций
A.5.1.2	Анализ политики информационной безопасности	Политика информационной безопасности организации должна быть подвергнута анализу и пересмотру через заданные промежутки времени или при появлении существенных изменений характеристик целей безопасности

A.6 Организация информационной безопасности		
A.6.1 Внутренняя организация Цель: Обеспечение управления информационной безопасностью в организации		
A.6.1.1	Обязанности руководства по обеспечению информационной безопасности	Руководство организации должно постоянно поддерживать заданный уровень информационной безопасности путем внедрения системы менеджмента, а также путем распределения обязанностей и ответственности персонала за ее обеспечение
A.6.1.2	Координация вопросов обеспечения информационной безопасности	Действия по обеспечению информационной безопасности должны координироваться представителями различных подразделений организации, имеющими соответствующие функции и должностные обязанности
A.6.1.3	Распределение обязанностей по обеспечению информационной безопасности	Обязанности персонала по обеспечению информационной безопасности должны быть четко определены
A.6.1.4	Процедура получения разрешения на использование средств обработки информации	Руководство должно определить и внедрить процедуры получения разрешения на использование новых средств обработки информации
A.6.1.5	Соглашения о соблюдении конфиденциальности	Руководство организации должно определять условия конфиденциальности или вырабатывать соглашения о неразглашении информации в соответствии с целями защиты информации и регулярно их пересматривать
A.6.1.6	Взаимодействие с компетентными органами	Руководство организации должно поддерживать взаимодействие с соответствующими компетентными органами

A.6.1.7	Взаимодействие с ассоциациями и профессиональными группами	Руководство организации должно поддерживать соответствующее взаимодействие с профессиональными группами, ассоциациями и участвовать (организовывать) в конференциях (форумах) специалистов в области информационной безопасности
A.6.1.8	Независимая проверка (аудит) информационной безопасности	Порядок организации и управления информационной безопасностью и ее реализация (например, изменение целей и мер управления, политики, процессов и процедур обеспечения информационной безопасности) должны быть подвергнуты независимой проверке (аудиту) через определенные промежутки времени или при появлении существенных изменений в способах реализации мер безопасности
A.6.2 Обеспечение безопасности при наличии доступа сторонних организаций к информационным системам Цель: Поддерживать безопасность информации и средств обработки информации организации при наличии доступа к ним сторонних организаций в процессах обработки и передачи этой информации		
A.6.2.1	Определение рисков, связанных со сторонними организациями	Перед предоставлением доступа сторонним организациям к информации и средствам ее обработки в процессе деятельности организации необходимо определять возможные риски для информации и средств ее обработки и реализовывать соответствующие им меры безопасности
A.6.2.2	Рассмотрение вопросов безопасности при работе с клиентами	Перед предоставлением клиентам права доступа к информации или активам организации необходимо определить и внедрить меры безопасности
A.6.2.3	Рассмотрение требований безопасности в соглашениях со сторонними организациями	Соглашения со сторонними организациями должны содержать все требования безопасности, включающие в себя правила доступа к процессам обработки, передачи информации или к управлению информацией или средствами обработки информации организации, а также и в случае приобретения дополнительных программных продуктов или организации сервисного обслуживания средств обработки информации

A.7 Управление активами		
A.7.1 Ответственность за защиту активов организации Цель: Обеспечивать соответствующую защиту активов организации		
A.7.1.1	Инвентаризация активов	Опись всех важных активов организации должна быть составлена и актуализирована
A.7.1.2	Владение активами	Вся информация и активы, связанные со средствами обработки информации, должны иметь назначенного во владение[1)] представителя организации

[1)] Термин "владелец" (owner) определен как лицо или организация, на которую возложена установленная ответственность управления по контролю производства, разработке, поддержке, использованию и безопасности активов. Термин "владелец" не означает, что данное лицо фактически имеет права собственности на этот актив.

A.7.1.3	Приемлемое использование активов	Правила безопасного использования информации и активов, связанных со средствами обработки информации, должны быть определены, документированы и реализованы
A.7.2 Классификация информации Цель: Обеспечить уверенность в том, что информация защищена на надлежащем уровне		
A.7.2.1	Основные принципы классификации	Информация должна быть классифицирована исходя из правовых требований, ее конфиденциальности, а также ценности и критичности для организации
A.7.2.2	Маркировка и обработка информации	В соответствии с принятой в организации системой классификации должна быть разработана и реализована совокупность процедур маркировки и обработки информации

A.8 Правила безопасности, связанные с персоналом		
A.8.1 Перед трудоустройством[1)] [1)] Под словом "трудоустройство" (employment) здесь поняты следующие ситуации: прием на работу (временную или постоянную), назначение на должность или перевод на другую должность, переоформление контрактов или аннулирование каких-либо из этих ситуаций. Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации осознают свою ответственность и способны выполнять предусмотренные для них функции и снижать риск от воровства, мошенничества и нецелевого использования оборудования, а также от угроз безопасности информации		
A.8.1.1	Функции и обязанности персонала по обеспечению безопасности	Функции и обязанности персонала по обеспечению безопасности сотрудников, подрядчиков и пользователей сторонней организации должны быть определены и документированы в соответствии с требованиями информационной безопасности
A.8.1.2	Проверка при приеме на работу	Проверка всех кандидатов на постоянную работу, подрядчиков и пользователей сторонней организации должна быть проведена в соответствии с законами, инструкциями и правилами этики, с учетом требований бизнеса, характера информации, к которой будет осуществлен их доступ, и предполагаемых рисков
A.8.1.3	Условия трудового договора	Сотрудники, подрядчики и пользователи сторонней организации должны согласовать и подписать условия своего трудового договора, в котором установлены их ответственность и ответственность организации относительно информационной безопасности

А.8.2 Работа по трудовому договору Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации осведомлены об угрозах и проблемах информационной безопасности, об их ответственности и обязательствах, ознакомлены с правилами и обучены процедурам для поддержания мер безопасности организации при выполнении ими своих служебных обязанностей и для снижения риска человеческого фактора для информационной безопасности		
А.8.2.1	Обязанности руководства	Руководство организации должно требовать, чтобы сотрудники, подрядчики и пользователи сторонней организации были ознакомлены с правилами и процедурами обеспечения мер безопасности в соответствии с установленными требованиями
А.8.2.2	Осведомленность, обучение и переподготовка в области информационной безопасности	Все сотрудники организации и, при необходимости, подрядчики и пользователи сторонних организаций должны проходить соответствующее обучение и переподготовку в целях регулярного получения информации о новых требованиях правил и процедур организации безопасности, необходимых для выполнения ими должностных функций
А.8.2.3	Дисциплинарная практика	К сотрудникам, совершившим нарушение требований безопасности, должна быть применена дисциплинарная практика, установленная в организации
А.8.3 Увольнение или изменение трудового договора Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации уведомлены об увольнении или изменении условий трудового договора в соответствии с установленным порядком		
А.8.3.1	Ответственность по окончании действия трудового договора	Ответственность по окончании действия трудового договора должна быть четко определена и установлена
А.8.3.2	Возврат активов	Сотрудники, подрядчики и пользователи сторонней организации обязаны вернуть все активы организации, находящиеся в их пользовании (владении), по истечении срока действия трудового договора или соглашения (увольнение)
А.8.3.3	Аннулирование прав доступа	Права доступа к информации и средствам обработки информации сотрудников, подрядчиков и пользователей сторонней организации должны быть аннулированы или уточнены по окончании действия трудового договора (увольнение)

A.9 Физическая защита и защита от воздействия окружающей среды		
A.9.1 Охраняемые зоны Цель: Предотвращать несанкционированные физический доступ, повреждение и воздействия на помещения и информацию организации		
A.9.1.1	Периметр охраняемой зоны	Для защиты зон, где имеются информация и средства обработки информации, должны быть использованы периметры охраняемых зон (барьеры, такие как стены, проходные, оборудованные средствами контроля входа по идентификационным карточкам, или, где предусмотрен, контроль сотрудника регистрационной стойки)
A.9.1.2	Контроль доступа в охраняемую зону	Охраняемая зона должна быть защищена соответствующими средствами контроля входа, предполагающими обеспечить уверенность в том, что только авторизованный персонал может получить доступ в зону
A.9.1.3	Обеспечение безопасности зданий, производственных помещений и оборудования	Требования к обеспечению физической безопасности зданий, производственных помещений и оборудования должны быть разработаны и реализованы
A.9.1.4	Защита от внешних угроз и угроз со стороны окружающей среды	Требования к обеспечению физической защиты зданий, производственных помещений и оборудования от нанесения ущерба в результате пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других природных и антропогенных факторов должны быть разработаны и реализованы
A.9.1.5	Выполнение работ в охраняемых зонах	Требования по физической защите и рекомендации по выполнению работ в охраняемых зонах должны быть разработаны и реализованы в инструкциях
A.9.1.6	Зоны общественного доступа, приема и отгрузки материальных ценностей	Места доступа, такие как зоны приема, отгрузки материальных ценностей и другие места, где неавторизованные лица могут проникнуть в помещения, должны быть под контролем и, по возможности, должны быть изолированы от средств обработки информации во избежание несанкционированного доступа

A.9.2 Безопасность оборудования Цель: Предотвращать потерю, повреждение, хищение или компрометацию активов и прекращение деятельности организации		
A.9.2.1	Размещение и защита оборудования	Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от воздействия окружающей среды и возможности несанкционированного доступа
A.9.2.2	Вспомогательные услуги	Оборудование необходимо защищать от перебоев в подаче электроэнергии и других сбоев, связанных с отказами в обеспечении вспомогательных услуг
A.9.2.3	Безопасность кабельной сети	Силовые и телекоммуникационные кабельные сети, по которым передаются данные или поддерживаются информационные услуги, необходимо защищать от перехвата информации или повреждения
A.9.2.4	Техническое обслуживание оборудования	Должно проводиться надлежащее регулярное техническое обслуживание оборудования для обеспечения его непрерывной работоспособности и сохранности
A.9.2.5	Обеспечение безопасности оборудования, используемого вне помещений организации	При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, должны быть учтены различные риски, связанные с работой вне помещений организации
A.9.2.6	Безопасная утилизация или повторное использование оборудования	Все компоненты оборудования, содержащие носители данных, должны быть проверены с целью удостовериться в том, что любые конфиденциальные данные и лицензионное программное обеспечение были удалены или скопированы безопасным образом до их утилизации (списания)
A.9.2.7	Вынос имущества с территории организации	Оборудование, информацию или программное обеспечение допускается выносить из помещения организации только на основании соответствующего разрешения

A.10 Управление средствами коммуникаций и их функционированием		
A.10.1 Эксплуатация средств и ответственность Цель: Обеспечить надлежащее и безопасное функционирование средств обработки информации		
A.10.1.1	Документирование операционных процедур эксплуатации	Операционные процедуры должны документироваться, поддерживаться и быть доступными для всех авторизованных пользователей
A.10.1.2	Управление изменениями	Изменения в конфигурациях средств обработки информации и системах должны быть контролируемыми
A.10.1.3	Разграничение обязанностей	Обязанности и области ответственности должны быть разграничены в целях снижения возможностей несанкционированной или непреднамеренной модификации, или нецелевого использования активов организации
A.10.1.4	Разграничение средств разработки, тестирования и эксплуатации	Средства разработки, тестирования и эксплуатации должны быть разграничены в целях снижения риска несанкционированного доступа или изменения операционной системы
A.10.2 Управление поставкой услуг лицами и/или сторонними организациями Цель: Реализовать и поддерживать требуемый уровень информационной безопасности и оказания услуг в соответствии с договорами об оказании услуг сторонними организациями (внешними лицами и/или организациями)		
A.10.2.1	Оказание услуг	Должна быть обеспечена уверенность в том, что меры управления информационной безопасностью, включенные в договор об оказании услуг сторонней организации, реализованы, функционируют и поддерживаются сторонней организацией
A.10.2.2	Мониторинг и анализ услуг, оказываемых сторонними лицами и/или организациями	Необходимо регулярно проводить мониторинг, аудит и анализ услуг, отчетов и актов, обеспечиваемых сторонней организацией
A.10.2.3	Изменения при оказании сторонними организациями услуг по обеспечению безопасности	Изменения при оказании услуг по обеспечению безопасности, включая внедрение и совершенствование существующих требований, процедур и мер обеспечения информационной безопасности, должны быть управляемыми с учетом оценки критичности систем и процессов бизнеса, а также результатов переоценки рисков

A.10.3 Планирование производительности и загрузки систем Цель: Свести к минимуму риск сбоев в работе систем		
A.10.3.1	Управление производительностью	Необходимо осуществлять прогнозирование, мониторинг и корректировку потребности мощности системы для обеспечения требуемой ее производительности
A.10.3.2	Приемка систем	Должны быть определены критерии принятия новых и модернизированных информационных систем, новых версий программного обеспечения, а также проведено тестирование систем в процессе их разработки и приемки
A.10.4 Защита от вредоносного кода и мобильного кода Цель: Защищать целостность программного обеспечения и массивов информации		
A.10.4.1	Меры защиты от вредоносного кода	Должны быть реализованы меры по обнаружению, предотвращению проникновения и восстановлению после проникновения вредоносного кода, а также должны быть установлены процедуры обеспечения соответствующего оповещения пользователей
A.10.4.2	Меры защиты от мобильного кода	Там, где разрешено использование мобильного кода, конфигурация системы должна обеспечивать уверенность в том, что авторизованный мобильный код функционирует в соответствии с четко определенной политикой безопасности, а исполнение операции с использованием неавторизованного мобильного кода будет предотвращено
A.10.5 Резервирование Цель: Поддерживать целостность и доступность информации и средств обработки информации		
A.10.5.1	Резервирование информации	Резервные копии информации и программного обеспечения должны создаваться, проверяться и тестироваться на регулярной основе в соответствии с принятыми требованиями резервирования

A.10.6 Управление безопасностью сети Цель: Обеспечить защиту информации в сетях и защиту поддерживающей инфраструктуры		
A.10.6.1	Средства контроля сети	Сети должны быть адекватно управляемыми и контролируемыми в целях защиты от угроз и поддержания безопасности систем и приложений, использующих сеть, включая информацию, передаваемую по сетям
A.10.6.2	Безопасность сетевых сервисов	Меры обеспечения безопасности, уровни обслуживания для всех сетевых услуг и требования управления должны быть определены и включены в любой договор о сетевых услугах независимо от того, предоставляются ли эти услуги своими силами или сторонней организацией
A.10.7 Обращение с носителями информации Цель: Предотвратить несанкционированное разглашение, модификацию, удаление или уничтожение активов и прерывание бизнес-процессов		
A.10.7.1	Управление съемными носителями информации	Для управления съемными носителями информации должны существовать соответствующие процедуры
A.10.7.2	Утилизация носителей информации	Носители информации, когда в них больше нет необходимости, должны быть надежно и безопасно утилизированы с помощью формализованных процедур
A.10.7.3	Процедуры обработки информации	Для обеспечения защиты информации от несанкционированного раскрытия или неправильного использования необходимо установить процедуры обработки и хранения информации
A.10.7.4	Безопасность системной документации	Системная документация должна быть защищена от несанкционированного доступа

A.10.8 Обмен информацией Цель: Поддерживать безопасность информации и программного обеспечения при обмене внутри организации и со сторонними организациями		
A.10.8.1	Политики и процедуры обмена информацией	Должны существовать формализованные процедуры, требования и меры контроля, обеспечивающие защиту обмена информацией при использовании связи всех типов
A.10.8.2	Соглашения по обмену информацией	Между организацией и сторонними организациями должны быть заключены соглашения по обмену информацией и программным обеспечением
A.10.8.3	Защита физических носителей информации при транспортировке	Носители информации должны быть защищены от несанкционированного доступа, неправильного использования или повреждения во время их транспортировки за пределами территории организации
A.10.8.4	Электронный обмен сообщениями	Информация, используемая в электронном обмене сообщениями, должна быть защищена надлежащим образом
A.10.8.5	Системы бизнес-информации	Требования и процедуры должны быть разработаны и внедрены для защиты информации, связанной с взаимодействием систем бизнес-информации
A.10.9 Услуги электронной торговли Цель: Обеспечить безопасность услуг электронной торговли и их безопасное использование		
A.10.9.1	Электронная торговля	Информация, используемая в электронной торговле, проходящая по общедоступным сетям, должна быть защищена от мошенничества, оспаривания контрактов, а также от несанкционированного разглашения и модификации
A.10.9.2	Трансакции в режиме реального времени (on-line)	Информация, используемая в трансакциях в режиме реального времени (on-line), должна быть защищена для предотвращения неполной передачи, неправильной маршрутизации, несанкционированного изменения сообщений, несанкционированного разглашения, несанкционированного копирования или повторного воспроизведения сообщений
A.10.9.3	Общедоступная информация	Информация, предоставляемая через общедоступную систему, должна быть защищена от несанкционированной модификации

A.10.10 Мониторинг Цель: Обнаруживать несанкционированные действия, связанные с обработкой информации		
A.10.10.1	Ведение журналов аудита	Должны быть обеспечены ведение и хранение в течение определенного периода времени журналов аудита, регистрирующих действия пользователей, нештатные ситуации и события информационной безопасности, в целях помощи в будущих расследованиях и проведении мониторинга контроля доступа
A.10.10.2	Мониторинг использования средств обработки информации	Должны быть установлены процедуры, позволяющие вести мониторинг и регулярный анализ результатов мониторинга использования средств обработки информации
A.10.10.3	Защита информации журналов регистрации	Средства регистрации и информация журналов регистрации должны быть защищены от вмешательства и несанкционированного доступа
A.10.10.4	Журналы регистрации действий администратора и оператора	Действия системного администратора и системного оператора должны быть регистрируемыми
A.10.10.5	Регистрация неисправностей	Неисправности должны быть зарегистрированы, проанализированы и устранены
A.10.10.6	Синхронизация часов	Часы всех соответствующих систем обработки информации в пределах организации или охраняемой зоны должны быть синхронизированы с помощью единого источника точного времени
A.11 Контроль доступа		
A.11.1 Бизнес-требования к контролю доступа Цель: Контролировать доступ к информации		
A.11.1.1	Политика контроля доступа	Политика контроля доступа должна быть установлена и документирована с учетом потребностей бизнеса и безопасности информации

A.11.2 Управление доступом пользователей Цель: Предотвратить несанкционированный доступ пользователей к информационным системам и обеспечить авторизованный доступ пользователей к этим системам		
A.11.2.1	Регистрация пользователей	Должна быть установлена формализованная процедура регистрации и снятия с регистрации пользователей для предоставления и отмены доступа ко всем информационным системам и услугам
A.11.2.2	Управление привилегиями	Предоставление и использование привилегий должно быть ограниченным и контролируемым
A.11.2.3	Управление паролями пользователей	Предоставление паролей должно быть контролируемым посредством формализованного процесса управления
A.11.2.4	Пересмотр прав доступа пользователей	Руководство должно периодически осуществлять пересмотр прав доступа пользователей, используя формализованный процесс
A.11.3 Ответственность пользователей Цель: Предотвращать несанкционированный доступ пользователей, а также компрометацию или кражу информации и средств обработки информации		
A.11.3.1	Использование паролей	Пользователи должны соблюдать правила безопасности при выборе и использовании паролей
A.11.3.2	Оборудование, оставленное пользователем без присмотра	Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра
A.11.3.3	Правила "чистого стола" и "чистого экрана"	Должны быть приняты правила "чистого стола" для документов на бумажных носителях и сменных носителей данных, а также правила "чистого экрана" для средств обработки информации

A.11.4 Контроль сетевого доступа Цель: Предотвратить несанкционированный доступ к сетевым сервисам		
A.11.4.1	Политика в отношении использования сетевых услуг	Пользователям следует предоставлять доступ только к тем услугам, по отношению к которым они специально были авторизованы
A.11.4.2	Аутентификация пользователей для внешних соединений	Для контроля доступа удаленных пользователей должны быть применены соответствующие методы аутентификации
A.11.4.3	Идентификация оборудования в сетях	Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений, осуществляемых с определенных мест и с определенным оборудованием
A.11.4.4	Защита диагностических и конфигурационных портов при удаленном доступе	Физический и логический доступ к портам конфигурации и диагностики должен быть контролируемым
A.11.4.5	Принцип разделения в сетях	В сетях должны быть применены принципы разделения групп информационных услуг, пользователей и информационных систем
A.11.4.6	Контроль сетевых соединений	Подключение пользователей к совместно используемым сетям, особенно к тем, которые выходят за территорию организации, необходимо ограничивать в соответствии с политикой контроля доступа и требованиями бизнес-приложений (см. A.11.1)
A.11.4.7	Контроль маршрутизации в сети	Должны быть внедрены средства управления и контроля маршрутизации в сети с целью исключить нарушения правил контроля доступа для бизнес-приложений, вызываемые соединениями и потоками информации

A.11.5 Контроль доступа к операционной системе Цель: Предотвратить несанкционированный доступ к операционным системам		
A.11.5.1	Безопасные процедуры регистрации	Контроль доступа к операционным системам должен быть обеспечен безопасной процедурой регистрации
A.11.5.2	Идентификация и аутентификация пользователя	Все пользователи должны иметь уникальные идентификаторы (ID) только для персонального использования, а для подтверждения заявленной личности пользователя должны быть выбраны подходящие методы аутентификации
A.11.5.3	Система управления паролями	Системы управления паролями должны быть интерактивными и обеспечивать высокое качество паролей
A.11.5.4	Использование системных утилит	Использование системных утилит, которые могут преодолеть средства контроля операционных систем и приложений, необходимо ограничивать и строго контролировать
A.11.5.5	Периоды бездействия в сеансах связи	Необходимо обеспечить завершение сеансов связи после определенного периода бездействия
A.11.5.6	Ограничение времени соединения	Ограничение времени соединения должно быть использовано для обеспечения дополнительной безопасности
A.11.6 Контроль доступа к прикладным системам и информации Цель: Предотвратить несанкционированный доступ к прикладным системам и информации		
A.11.6.1	Ограничения доступа к информации	Доступ к информации и функциям прикладных систем пользователей и обслуживающего персонала должен быть предоставлен только в соответствии с определенными политиками контроля доступа
A.11.6.2	Изоляция систем, обрабатывающих важную информацию	Системы, обрабатывающие важную информацию, должны иметь выделенную (изолированную) вычислительную среду
A.11.7 Работа с переносными устройствами и работа в дистанционном режиме Цель: Обеспечить информационную безопасность при использовании переносных устройств и средств, необходимых для работы в дистанционном режиме		
A.11.7.1	Работа с переносными устройствами	Необходимо иметь в наличии формализованную политику для защиты от рисков при использовании переносных устройств
A.11.7.2	Работа в дистанционном режиме	Для работы в дистанционном режиме необходимо разработать и реализовать политику, оперативные планы и процедуры

A.12 Разработка, внедрение и обслуживание информационных систем		
A.12.1 Требования к безопасности информационных систем Цель: Обеспечить уверенность в том, что безопасность является неотъемлемым свойством внедряемых информационных систем, и обеспечить выполнение требований безопасности при разработке и эксплуатации систем		
A.12.1.1	Анализ и детализация требований безопасности	В формулировках требований бизнеса для новых информационных систем или совершенствования существующих должны быть детализированы требования безопасности
A.12.2 Правильная обработка данных в приложениях Цель: Предотвратить ошибки, потерю, несанкционированную модификацию или неправильное использование информации в приложениях		
A.12.2.1	Проверка достоверности входных данных	Входные данные для приложений должны быть подвергнуты процедуре подтверждения с целью установления их достоверности
A.12.2.2	Контроль обработки данных в приложениях	Для обнаружения искажений (ошибок или преднамеренных действий) при обработке информации в требования к функциям приложений должны быть включены требования по выполнению контрольных проверок
A.12.2.3	Целостность сообщений	Должны быть определены требования для обеспечения аутентичности и защиты целостности сообщений в приложениях, а также реализованы соответствующие средства контроля
A.12.2.4	Подтверждение достоверности выходных данных	Данные, выводимые из приложения, необходимо подвергать проверке на корректность, чтобы обеспечить уверенность в том, что обработка информации выполнена правильно

A.12.3 Криптографические средства защиты Цель: Защищать конфиденциальность, аутентичность или целостность информации криптографическими средствами		
A.12.3.1	Политика использования криптографических средств защиты	Должны быть разработаны и внедрены правила использования криптографических средств защиты информации
A.12.3.2	Управление ключами	Для реализации организацией криптографических методов защиты должна быть использована система управления ключами
A.12.4 Безопасность системных файлов Цель: Обеспечить безопасность системных файлов		
A.12.4.1	Контроль программного обеспечения, находящегося в промышленной эксплуатации	Необходимо обеспечить контроль за процессом внедрения программного обеспечения в промышленную эксплуатацию
A.12.4.2	Защита данных тестирования системы	Данные тестирования следует тщательно отбирать, защищать и контролировать
A.12.4.3	Контроль доступа к исходным кодам	Доступ к исходным кодам должен быть ограничен

A.12.3 Криптографические средства защиты Цель: Защищать конфиденциальность, аутентичность или целостность информации криптографическими средствами		
A.12.3.1	Политика использования криптографических средств защиты	Должны быть разработаны и внедрены правила использования криптографических средств защиты информации
A.12.3.2	Управление ключами	Для реализации организацией криптографических методов защиты должна быть использована система управления ключами
A.12.4 Безопасность системных файлов Цель: Обеспечить безопасность системных файлов		
A.12.4.1	Контроль программного обеспечения, находящегося в промышленной эксплуатации	Необходимо обеспечить контроль за процессом внедрения программного обеспечения в промышленную эксплуатацию
A.12.4.2	Защита данных тестирования системы	Данные тестирования следует тщательно отбирать, защищать и контролировать
A.12.4.3	Контроль доступа к исходным кодам	Доступ к исходным кодам должен быть ограничен

A.12.5 Безопасность в процессах разработки и поддержки		
Цель: Поддерживать безопасность программного обеспечения прикладных систем и содержащейся в них информации		
A.12.5.1	Процедуры контроля изменений	Внесение изменений должно быть проверено с использованием соответствующих формализованных процедур контроля изменений
A.12.5.2	Технический анализ прикладных систем после внесения изменений в операционные системы	При внесении изменений в операционные системы необходимо провести анализ и тестирование критичных бизнес-приложений с целью удостовериться в отсутствии негативного влияния на работу и безопасность организации
A.12.5.3	Ограничения на внесение изменений в пакеты программ	Необходимо избегать модификаций пакетов программ, а все требуемые изменения должны подлежать строгому контролю
A.12.5.4	Утечка информации	Возможности для утечки информации должны быть предотвращены
A.12.5.5	Разработка программного обеспечения с привлечением сторонних организаций	Разработка программного обеспечения с привлечением сторонних организаций должна проводиться под контролем и при мониторинге организации
A.12.6 Менеджмент технических уязвимостей		
Цель: Снизить риски, являющиеся результатом использования опубликованных технических уязвимостей		
A.12.6.1	Управление техническими уязвимостями	Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать опасность таких уязвимостей и принимать соответствующие меры по устранению связанного с ними риска

A.13 Управление инцидентами информационной безопасности		
A.13.1 Оповещение о нарушениях и недостатках информационной безопасности Цель: Обеспечить оперативность оповещения о событиях информационной безопасности и нарушениях, связанных с информационными системами, а также своевременность корректирующих действий		
A.13.1.1	Оповещение о случаях нарушения информационной безопасности	О случаях нарушения информационной безопасности следует сообщать по соответствующим каналам управления незамедлительно, насколько это возможно
A.13.1.2	Оповещение о недостатках безопасности	Все сотрудники, подрядчики и пользователи сторонних организаций, пользующиеся информационными системами и услугами, должны незамедлительно сообщать о любых замеченных или предполагаемых нарушениях безопасности в системах или услугах
A.13.2 Управление инцидентами информационной безопасности и его усовершенствование Цель: Обеспечить последовательный и эффективный подход к управлению инцидентами информационной безопасности		
A.13.2.1	Ответственность и процедуры	Должны быть установлены ответственность руководства и процедуры, позволяющие обеспечить быстрое, эффективное и последовательное реагирование на инциденты информационной безопасности
A.13.2.2	Извлечение уроков из инцидентов информационной безопасности	Должны быть определены механизмы, позволяющие вести мониторинг и регистрацию инцидентов информационной безопасности по типам, объемам и стоимостям
A.13.2.3	Сбор доказательств	На случай, если инцидент информационной безопасности может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, информация должна быть собрана, сохранена и представлена согласно правилам оформления доказательств, изложенным в соответствующих документах

A.14 Управление непрерывностью бизнеса		
A.14.1 Вопросы информационной безопасности управления непрерывностью бизнеса Цель: На случай, если инцидент информационной безопасности может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, информация должна быть собрана, сохранена и представлена согласно правилам оформления доказательств, изложенным в соответствующих документах		
A.14.1.1	Включение информационной безопасности в процесс управления непрерывностью бизнеса	Должен быть разработан и поддержан управляемый процесс обеспечения непрерывности бизнеса во всей организации с учетом требований информационной безопасности, необходимых для обеспечения непрерывности бизнеса организации
A.14.1.2	Непрерывность бизнеса и оценка риска	События, которые могут стать причиной прерывания бизнес-процессов, должны быть связаны с оценками вероятности и степени воздействия таких прерываний, а также с их последствиями для информационной безопасности
A.14.1.3	Разработка и внедрение планов непрерывности бизнеса, включающих в себя информационную безопасность	Должны быть разработаны и внедрены планы для поддержки или восстановления работы и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или отказа критических бизнес-процессов
A.14.1.4	Структура плана обеспечения непрерывности бизнеса	Должна быть создана единая структура планов непрерывности бизнеса, позволяющая обеспечить непротиворечивость всех планов для последовательного выполнения всех требований к информационной безопасности и для расстановки приоритетов при тестировании и обслуживании
A.14.1.5	Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса	Планы по обеспечению непрерывности бизнеса должны подлежать регулярному пересмотру и обновлению с целью обеспечить их актуальность и эффективность

A.15 Соответствие требованиям		
A.15.1 Соответствие правовым требованиям Цель: Предотвращать любые нарушения норм уголовного и гражданского права, требований, установленных нормативно-правовыми актами, регулирующими органами или договорными обязательствами, а также требований безопасности		
A.15.1.1	Определение применимых норм	Все применимые нормы, установленные законодательством и исполнительными органами власти, требования договорных обязательств и порядок их выполнения следует четко определить, документировать и поддерживать на актуальном уровне для каждой информационной системы и организации
A.15.1.2	Права на интеллектуальную собственность	Должны быть внедрены соответствующие процедуры для применения законодательных, регулирующих и контрактных требований к используемым материалам с учетом прав на интеллектуальную собственность, а также прав на использование программных продуктов, являющихся предметом частной собственности
A.15.1.3	Защита учетных записей организации	Важные учетные записи организации должны быть защищены от утраты, разрушения и фальсификации в соответствии с требованиями, установленными законами, документами органов исполнительной власти, контрактами и требованиями бизнеса
A.15.1.4	Защита данных и конфиденциальность персональной информации	Защита данных и конфиденциальность персональной информации должны быть обеспечены в соответствии с требованиями законов, нормативных актов и, где это применимо, в соответствии с положениями контрактов
A.15.1.5	Предотвращение нецелевого использования средств обработки информации	Должны быть применены меры контроля для предотвращения нецелевого использования средств обработки информации
A.15.1.6	Регулирование использования средств криптографической защиты	Средства криптографической защиты должны быть использованы в соответствии с законами, нормативными актами и соответствующими соглашениями

A.15.2 Соответствие политикам и стандартам безопасности и техническое соответствие требованиям безопасности Цель: Обеспечить соответствие систем организационным политикам и стандартам безопасности		
A.15.2.1	Соответствие политикам и стандартам безопасности	Руководители должны обеспечить, чтобы все процедуры безопасности в их сфере ответственности были выполнены правильно и соответствовали политикам и стандартам безопасности
A.15.2.2	Проверка технического соответствия требованиям безопасности	Информационные системы следует регулярно проверять на соответствие требованиям стандартов безопасности
A.15.3 Вопросы аудита информационных систем Цель: Повышение эффективности процесса аудита информационных систем и снижение негативного влияния, связанного с данным процессом		
A.15.3.1	Меры управления аудитом информационных систем	Требования и процедуры аудита, включающие в себя проверки операционных систем, необходимо тщательно планировать и согласовывать, чтобы свести к минимуму риск прерывания бизнес-процессов
A.15.3.2	Защита инструментальных средств аудита информационных систем	Доступ к инструментальным средствам аудита информационных систем необходимо защищать для предотвращения любой возможности их неправильного использования или компрометации