ТЕМА 2. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЧАСТНЫЕ ПОЛИТИКИ

Профессор, дтн Минзов А.С.

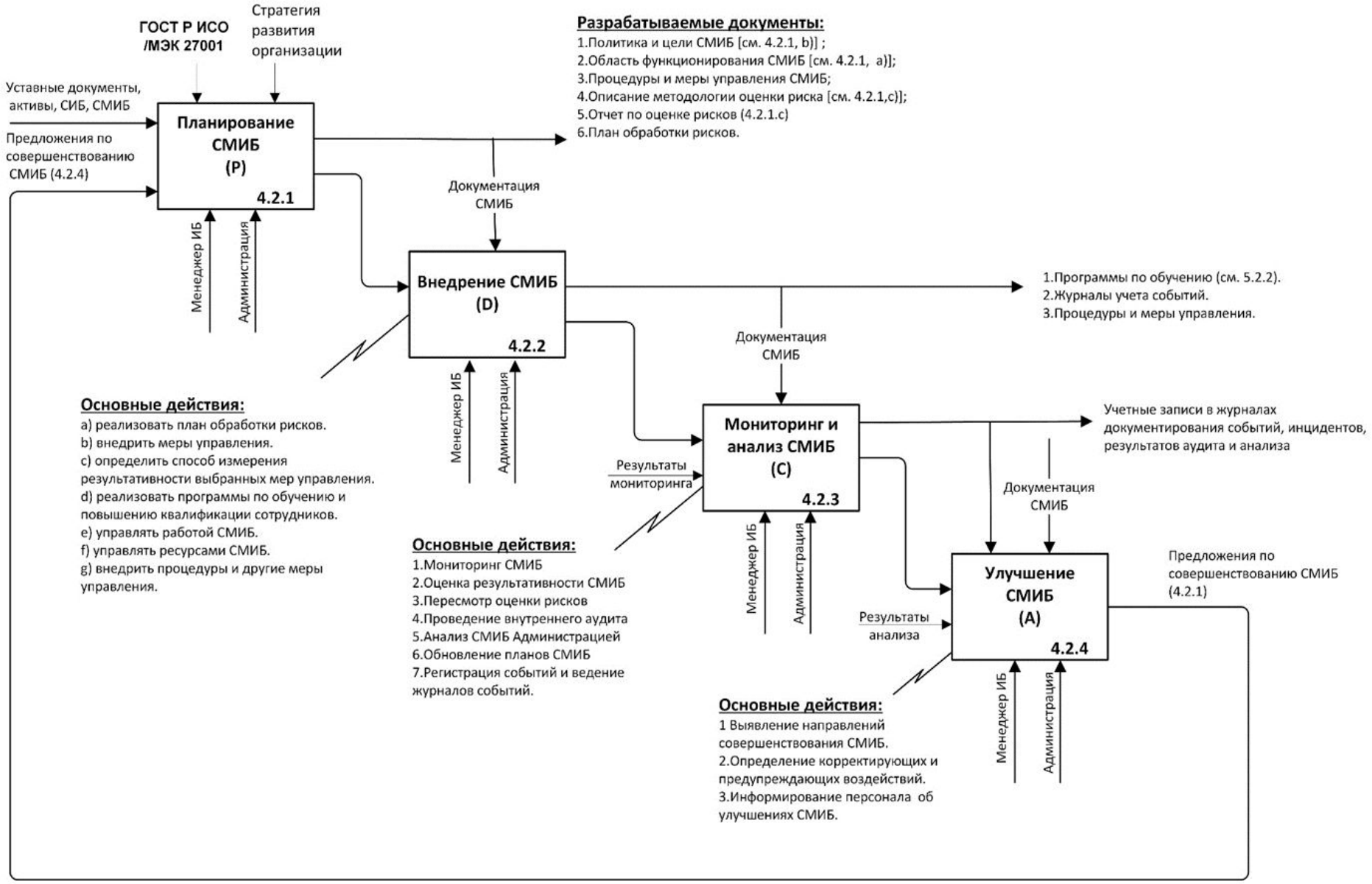
Содержание

1. Введение
2. Политика безопасности: назначение, структура и содержание
3. Методика разработки частных политик.
4. Заключение

Введение

- Система стандартов ГОСТ р ИСО/МЭК 27001 и ГОСТ р ИСО/МЭК 27002 и их роль в реализации процессного подхода к информационной безопасности.

1.Последовательность разработки и внедрения СМИБ


ГОСТ Р ИСО /МЭК 27001
Стратегия развития организации
Уставные документы, активы, СИБ, СМИБ
Предложения по совершенствованию СМИБ (4.2.4)
Планирование СМИБ (P)
4.2.1
Менеджер ИБ
Администрация
Разрабатываемые документы:
1.Политика и цели СМИБ [см. 4.2.1, b)] ;
2.Область функционирования СМИБ [см. 4.2.1, a)];
3.Процедуры и меры управления СМИБ;
4.Описание методологии оценки риска [см. 4.2.1,c)];
5.Отчет по оценке рисков (4.2.1.c)
6.План обработки рисков.
Документация СМИБ
Внедрение СМИБ (D)
4.2.2
1.Программы по обучению (см. 5.2.2).
2.Журналы учета событий.
3.Процедуры и меры управления.
Основные действия:
a) реализовать план обработки рисков.
b) внедрить меры управления.
c) определить способ измерения результативности выбранных мер управления.
d) реализовать программы по обучению и повышению квалификации сотрудников.
e) управлять работой СМИБ.
f) управлять ресурсами СМИБ.
g) внедрить процедуры и другие меры управления.
Документация СМИБ
Мониторинг и анализ СМИБ (C)
4.2.3
Учетные записи в журналах документирования событий, инцидентов, результатов аудита и анализа
Результаты мониторинга
Документация СМИБ
Основные действия:
1.Мониторинг СМИБ
2.Оценка результативности СМИБ
3.Пересмотр оценки рисков
4.Проведение внутреннего аудита
5.Анализ СМИБ Администрацией
6.Обновление планов СМИБ
7.Регистрация событий и ведение журналов событий.
Улучшение СМИБ (A)
4.2.4
Предложения по совершенствованию СМИБ (4.2.1)
Результаты анализа
Основные действия:
1 Выявление направлений совершенствования СМИБ.
2.Определение корректирующих и предупреждающих воздействий.
3.Информирование персонала об улучшениях СМИБ.

Разработка и внедрение СМИБ
(вариант)

1. **Обследование компании**

1.1. Выбор области функционирования системы управления информационной безопасностью

1.2. Идентификация информационных активов в рамках области действия СМИБ

1.3. Сбор и анализ информации о применяемых в компании средствах и методах защиты

2. **Оценка и анализ рисков информационной безопасности компании**

2.1. Разработка и согласование методики анализа рисков безопасности

2.2. Проведение оценки рисков безопасности

2.3. Разработка рекомендаций по совершенствованию нормативно-методического и технологического обеспечения, направленного на минимизацию рисков информационной безопасности

Разработка и внедрение СМИБ

3. Разработка проекта по внедрению системы управления информационной безопасностью

3.1. Разработка/корректировка политики информационной безопасности компании

3.2. Разработка/корректировка политик и процедур СМИБ

3.3. Разработка технического проекта по реализации комплексной системы защиты информации компании

4. Внедрение системы управления информационной безопасностью

4.1. Обучение сотрудников компании в соответствии с разработанными документами (пп. 3.1, 3.2)

4.2. Установка/настройка средств защиты информации в соответствии с техническим проектом (п. 3.3)

Разработка и внедрение СМИБ

5. **Общий аудит по окончанию работ**

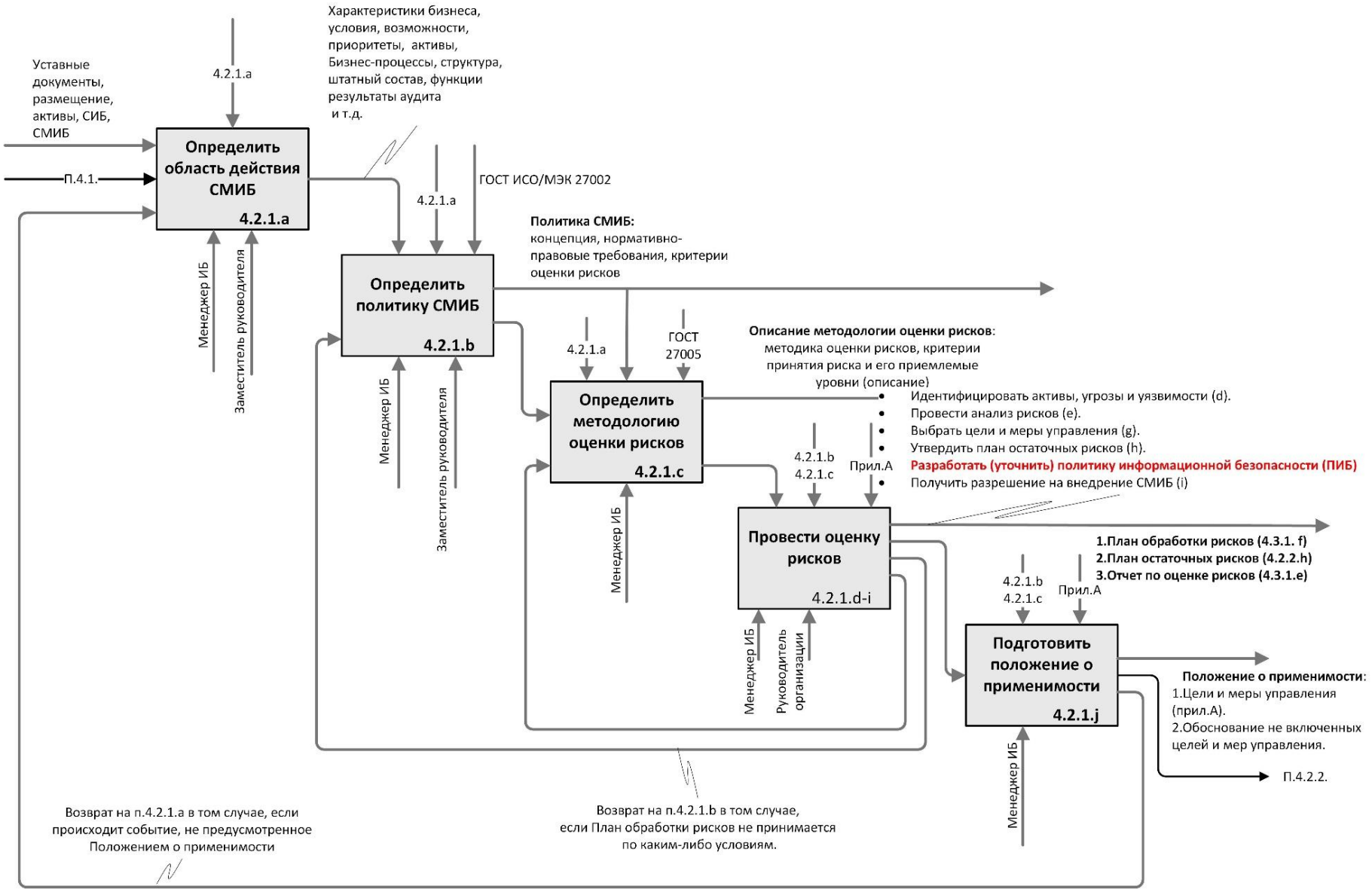
5.1. Контрольный аудит

5.2. Корректировка и устранение недостатков

6. **Подготовительные работы к проведению сертификации на соответствие ISO 27001**

6.1. Оформление необходимых документов

6.2. Подача заявки в представительство BSI



УЗЕЛ:	4.2.1	ЗАГОЛОВОК:	Процесс разработки СМИБ по ГОСТ ИСО/МЕК 27001	НОМЕР:	1

Содержание политики информационной безопасности (ПИБ)

ГОСТ ИСО/МЭК 27002-2012

Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

Термины и определения

- Политика информационной безопасности (ПИБ) — набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области ЗИ (их более 800 !).
- Частная ПИБ отражает набор правил в отношении одного из направлений защиты информации, например физической защиты информационных активов.

Структура ПИБ

Политика безопасности (ПИБ)

(раздел 5 ГОСТ Р ИСО/МЭК 27002-2012)

- Общие аспекты политики
- Организационные аспекты ИБ
- Менеджмент активов
- Физическая безопасность и защита от окружающей среды.
- Управление коммуникациями и работами
- Управление персоналом
- Управление доступом
- Приобретение и разработка ИС
- Менеджмент инцидентов
- Менеджмент непрерывности бизнеса
- Соответствие

Частные политики

1. Политика организации ИБ
2. Политика менеджмента активов
3. Политика безопасности, связанная с персоналом
4. Политика физической защиты и защиты от окружающей среды
5. Политика менеджмента коммуникаций и работ.
6. Политика управления доступом.
7. Политика разработки, приобретения и эксплуатации ИС.
8. Политика менеджмента инцидентов ИБ.
9. Политика непрерывности бизнеса.
10. Политика соответствия.

Общие аспекты политики

- Цель: обеспечить управление и поддержку руководством систему требований к СИБ в соответствие с требованиями бизнеса, нормами и законами.
- Политика включает документированный набор определенных требований к СИБ.
- Пересмотр ПИБ осуществляется в тех случаях, когда меняются требования к ИБ, меняются условия, изменяются методы управления и условия.

Требования к политике

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

Разделы политики (рекомендуемые)

1. Определение ИБ, целей и сферы действия.
2. Намерения руководства в сфере ИБ.
3. Меры и средства контроля и управления.
4. Распределение ролей и определение обязанностей сотрудников.
5. Краткое изложение основных политик.
6. Ссылки на нормативные и другие документы.

Пример политики (цели)

1. Цели

1.1. Распределить ответственность персонала и их полномочия в сфере защиты активов информационных систем ИББ.

1.2. Обеспечить защиту информационных активов ИББ МЭИ (ТУ):

при проведении учебного процесса с различными категориями студентов, слушателей, преподавателей и администрации;

- при организации и выполнении НИР;
- при работе в автоматизированной информационной системе вуза (ИРИС);
- при ведении информационного обмена по внутренним и внешним телекоммуникационным каналам связи (документооборот);
- при использовании ИНТЕРНЕТ как в часы занятий, так и в часы самостоятельной работы по проводным и беспроводным каналам связи.

Пример политики (Цели)

1.3. Оценить риски информационной безопасности и предложить рациональную стратегию их снижения, передачи или отказа от них.

1.4. Обеспечить ответственных за информационную безопасность ИББ достаточной информацией для расследования инцидентов информационной безопасности.

1.5. Защитить служебную и личную информацию студентов, преподавателей и научных сотрудников, размещенную в электронных библиотеках, личных архивах и на серверах ИББ в ИНТЕРНЕТ.

1.6. Создать обоснованные требования доверия к системе информационной безопасности ИББ со стороны пользователей.

1.7.Обеспечить безопасную работу с персональными данными студентов и слушателей.

1.8. Обеспечить непрерывный образовательный процесс пользователей, повышение его эффективности.

1.9. Обеспечить безопасность при проведении обучения со студентами по программе Capture the flag (CTF).

Пример политики (Угрозы)

Источниками угроз являются:

студенты, преподаватели, сотрудники, внешние пользователи, проявляющие интерес к информационным активам организации. Мотивы угроз могут быть различны от хищения интеллектуальной собственности до удовлетворения собственного любопытства.

Пример политики (Роли)

Студенты гуманитарных направлений подготовки.

Этот профиль имеет доступ к офисным приложениям в полном объеме, Виртуальному университету МЭИ, аналитических информационных систем (ИНТЕГРУМ, СПАРК, Галактика-ZOOM, Семантический архив), электронной библиотеке и энциклопедии безопасности (Wi-ki) и другому прикладному программному обеспечению, предустановленному заранее, и имеющему сертификаты подлинности. Кроме того, предоставляется доступ к ресурсам ИНТЕРНЕТ по протоколу http с фильтрацией трафика по социальным сетям, агрессивным и другим подобным порталам (база данных по этим порталам обновляется периодически). Обмен информацией между пользователями сети через специально организованные сетевые папки.

Условия обновления политики

- Изменения бизнес-процессов
- Изменения организационно -штатной структуры
- Появление инцидентов
- Изменение нормативной базы
- Появление новой чувствительной, критичной и конфиденциальной информации
- Увольнение персонала, реализующего политику
- …

Пример фрагмента политики информационной безопасности образовательного учреждения

1. Цели

1.1. Распределить ответственность персонала и их полномочия в сфере защиты активов информационных систем ИББ.

1.2. Обеспечить защиту информационных активов ИББ МЭИ (ТУ):

- **при проведении учебного процесса с различными категориями студентов, слушателей, преподавателей и администрации;**
- **при организации и выполнении НИР студентами, слушателями, аспирантами;**
- **при использовании ИНТЕРНЕТ как в часы занятий, так и в часы самостоятельной работы по проводным и беспроводным каналам связи.**

1.3. Обеспечить расследование инцидентов информационной безопасности.

1.4.Обеспечить безопасную работу с персональными данными студентов.

1.5. Обеспечить непрерывный образовательный процесс пользователей.

1.6. Обеспечить безопасность при проведении обучения со студентами по программе Capture the flag (CTF).

Принципы информационной безопасности (пример)

1. **Системность решений**, позволяющая рассматривать решения по защите информации как систему, с соответствующими ей свойствами.
2. Рациональность решений в сфере информационной безопасности, позволяющая при заданных ограничениях на затраты обеспечить наиболее полную защиту информационных активов.
3. Комплексность решений, проявляющаяся в интеграции различных подсистем в единую систему информационной безопасности.
4. Персональная авторизация и ответственность персонала за свои действия.
5. Неотказуемость персонала от неумышленных и умышленных действий, приводящих к возникновению инцидентов.
6. Возможность адаптации системы защиты к новым угрозам информационной безопасности.
7. Непрерывность образовательного и научного процесса.
8. Использование только лицензионного и свободно распространяемого программного обеспечения.

Частные политики информационной безопасности

Организация информационной безопасности (раздел 5 ГОСТ 27002)

А.6.1 Внутренняя организация

Цель: Обеспечение управления информационной безопасностью в организации

А.6.1.1 Обязанности руководства

А.6.1.2 Координация вопросов обеспечения информационной безопасности

А.6.1.3 Распределение обязанностей персонала (ролей) по информ.безопасн.

А.6.1.4 Процесс получения разрешения на использование средств обработки информации

А.6.1.5 Соглашения о соблюдении конфиденциальности

А.6.1.6 Взаимодействие с компетентными органами

А.6.1.7 Взаимодействие с ассоциациями и профессиональными группами

А.6.1.8 Независимая проверка (аудит) информационной безопасности

А.6.2 Обеспечение безопасности при наличии доступа сторонних организаций к информационным системам

А.6.2.1 Определение рисков, связанных со сторонними организациями

А.6.2.2 Рассмотрение вопросов безопасности при работе с клиентами

А.6.2.3 Требования безопасности в соглашениях со сторонними организациями

A.6.1 Внутренняя организация

A.6.1.1 Обязанности руководства

a) обеспечивать уверенность;
b) формулировать, анализировать и утверждать политику информационной безопасности;
c) анализировать эффективность реализации политики информационной безопасности;
d) обеспечивать четкое управление;
e) обеспечивать необходимые ресурсы;
f) утверждать определенные роли и ответственности;
д) инициировать планы и программы для поддержки осведомленности;

A.6.1.2 Координация вопросов обеспечения информационной безопасности

a)
b) определять способ устранения несоответствия;
c) утверждать методики и процессы обеспечения информационной безопасности;
d) выявлять значительные изменения угроз;
e) координировать реализацию мер и средств контроля;
f) эффективно способствовать осведомленности, обучению и тренингу в отношении информационной безопасности в рамках организации;
д) оценивать информацию, по выявленным инцидентам.

A.6.1.3 Распределение обязанностей персонала (ролей) по информ.безопасн.

a) активы и процессы (процедуры) безопасности должны быть четко определены;
b) необходимо назначить ответственных за каждый актив или процедуру безопасности;
c) уровни полномочий должны быть четко определены и документально оформлены.

A.6.1.4 Процесс получения разрешения на использование средств обработки информации

A.6.1 Внутренняя организация

A.6.1.5 Соглашения о соблюдении конфиденциальности

a) определение информации, подлежащей защите;
b) предполагаемый срок действия соглашения;
c) необходимые действия при окончании срока действия соглашения;
d) обязанности и действия лиц,
e) владение информацией;
f) разрешенное использование конфиденциальной информации и права лиц;
g) право подвергать аудиту и мониторингу;
h) процедуру предупреждения и сообщения о нарушениях;
i) условия возврата или уничтожения информации;
j) предполагаемые действия в случае нарушения соглашения.

A.6.1.6 Взаимодействие с компетентными органами

Особенности взаимодействия.

A.6.1.7 Взаимодействие с ассоциациями и профессиональными группами

Членство в специализированных группах или форумах

A.6.1.8 Независимая проверка (аудит) информационной безопасности

Особенности

A.6.2 Обеспечение безопасности при наличии доступа сторонних организаций к информационным системам

A.6.2.1 Определение рисков, связанных со сторонними организациями

a) средства обработки информации,

b) тип доступа к информации и средствам обработки информации: физический , логический, сетевой, вне места эксплуатации.

c) ценность и чувствительность используемой информации;

d) меры и средства контроля и управления,;

e) персонал сторонней организации;

f,) условия авторизоации ;

h) влияние непредоставления требуемого доступа сторонней организации;

i) инструкции и процедуры принятия мер в отношении инцидентов информационной безопасности;

j) правовые и нормативные требования, а также договорные обязательства;

k) влияние вышеназванных мер на интересы каких-либо других причастных сторон.

A.6.2 Обеспечение безопасности при наличии доступа сторонних организаций к информационным системам

A.6.2.2 Рассмотрение вопросов безопасности при работе с клиентами

a) защита активов

b) описание продукта или услуги, которые должны быть обеспечены;

c) различные причины, требования и преимущества, связанные с доступом клиента;

d) политика управления доступом

e) процедуры в отношении отчетности, уведомления и расследования неточностей в информации

f) описание каждой предоставляемой услуги;

д) определение необходимого и неприемлемого уровня обслуживания;

h) право на проведение мониторинга и отмену какой-либо деятельности,

i) соответствующие обязательства организации и клиента;

j) обязательства обеспечения правовым нормам.

A.6.2 Обеспечение безопасности при наличии доступа сторонних организаций к информационным системам

A.6.2.3 Требования безопасности в соглашениях со сторонними организациями

a) политика информационной безопасности;

b) меры и средства контроля и управления для обеспечения уверенности в защите активов, включая:

1) процедуры по защите активов организации

2) какие-либо меры и средства контроля и управления, а также инструменты необходимой физической защиты;

3) меры и средства контроля и управления

4) процедуры по определению компрометации активов;

5) конфиденциальность, целостность, доступность;

7) ограничения на копирование и разглашение информации;

c) тренинг пользователей и администраторов в отношении методов, процедур безопасности;

d) обеспечение осведомленности пользователей в отношении обязанностей и вопросов, связанных с информационной безопасностью;

e) обеспечение доставки персонала к месту работы, где это необходимо;

f) обязанности, касающиеся установки и сопровождения аппаратных средств и ПО;

д) четкая структура подотчетности и согласованные форматы представления отчетов;

h) ясный и определенный процесс менеджмента изменений;

i) политика управления доступом;

Управление активами (А.7)

А.7.1 Ответственность за защиту активов организации

Цель: Обеспечивать соответствующую защиту активов организации

А.7.1.1 Инвентаризация активов

А.7.1.2 Владение активами

А.7.1.3 Приемлемое использование активов

А.7.2 Классификация информации

Цель: Обеспечить уверенность в том, что информация защищена на надлежащем уровне

А.7.2.1 Основные принципы классификации

А.7.2.2 Маркировка и обработка информации

Правила безопасности, связанные с персоналом (раздел А.8)

А.8.1 Перед трудоустройством

Цель: Обеспечить уверенность в том, что сотрудники осознают свою ответственность и способны выполнять предусмотренные для них функции и снижать риск от угроз безопасности информации

А.8.1.1 Функции и обязанности персонала по обеспечению безопасности

А.8.1.2 Проверка при приеме на работу

А.8.1.3 Условия трудового договора

А.8.2 Работа по трудовому договору

Цель: Обеспечить уверенность в том, что сотрудники 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.

А.8.2.1 Обязанности руководства

А.8.2.2 Осведомленность, обучение и переподготовка в области информационной безопасности

А.8.2.3 Дисциплинарная практика

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

А.8.3.2 Возврат активов

А.8.3.3 Аннулирование прав доступа

Физическая защита и защита от воздействия окружающей среды (a.9)

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
A.9.1.2 Контроль доступа в охраняемую зону
A.9.1.3 Обеспечение безопасности зданий, производственных помещений и оборудования
A.9.1.4 Защита от внешних угроз и угроз со стороны окружающей среды
A.9.1.5 Выполнение работ в охраняемых зонах
A.9.1.6 Зоны общественного доступа, приема и отгрузки материальных ценностей

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
A.9.2.2 Вспомогательные услуги
A.9.2.3 Безопасность кабельной сети
A.9.2.4 Техническое обслуживание оборудования
A.9.2.5 Обеспечение безопасности оборудования, используемого вне помещений организации
A.9.2.6 Безопасная утилизация или повторное использование оборудования
A.9.2.7 Вынос имущества с территории организации

Управление средствами коммуникаций и их функционированием (а.10,1-6)

А.10.1 Эксплуатация средств и ответственность

Цель: Обеспечить надлежащее и безопасное функционирование средств обработки информации

А.10.1.1 Документирование операционных процедур эксплуатации

А.10.1.2 Управление изменениями

А.10.1.3 Разграничение обязанностей

А.10.1.4 Разграничение средств разработки, тестирования и эксплуатации

А.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)

А.10.2.1 Оказание услуг

А.10.2.2 Мониторинг и анализ услуг, оказываемых сторонними лицами и/или организациями

А.10.2.3 Изменения при оказании сторонними организациями услуг по обеспечению безопасности

А.10.3 Планирование производительности и загрузки систем

Цель: Свести к минимуму риск сбоев в работе систем

А.10.3.1 Управление производительностью

А.10.3.2 Приемка систем

А.10.4 Защита от вредоносного кода и мобильного кода

Цель: Защищать целостность программного обеспечения и массивов информации

А.10.4.1 Меры защиты от вредоносного кода

А.10.4.2 Меры защиты от мобильного кода

А.10.5 Резервирование

Цель: Поддерживать целостность и доступность информации и средств обработки информации

А.10.5.1 Резервирование информации

А.10.6 Управление безопасностью сети

Цель: Обеспечить защиту информации в сетях и защиту поддерживающей инфраструктуры

А.10.6.1 Средства контроля сети

А.10.6.2 Безопасность сетевых сервисов

Управление средствами коммуникаций и их функционированием (а.10,7-10)

А.10.7 Обращение с носителями информации

Цель: Предотвратить несанкционированное разглашение, модификацию, удаление или уничтожение активов и прерывание бизнес-процессов

А.10.7.1 Управление съемными носителями информации
А.10.7.2 Утилизация носителей информации
А.10.7.3 Процедуры обработки информации
А.10.7.4 Безопасность системной документации

А.10.8 Обмен информацией

Цель: Поддерживать безопасность информации и программного обеспечения при обмене внутри организации и со сторонними организациями

А.10.8.1 Политики и процедуры обмена информацией
А.10.8.2 Соглашения по обмену информацией
А.10.8.3 Защита физических носителей информации при транспортировке
А.10.8.4 Электронный обмен сообщениями
А.10.8.5 Системы бизнес- информации

А.10.9 Услуги электронной торговли

Цель: Обеспечить безопасность услуг электронной торговли и их безопасное использование

А.10.9.1 Электронная торговля
А.10.9.2 Трансакции в режиме реального времени (on-line)
А.10.9.3 Общедоступная информация

А.10.10 Мониторинг

Цель: Обнаруживать несанкционированные действия, связанные с обработкой информации

А.10.10.1 Ведение журналов аудита
А.10.10.2 Мониторинг использования средств обработки информации
А.10.10.3 Защита информации журналов регистрации
А.10.10.4 Журналы регистрации действий администратора и оператора
А.10.10.5 Регистрация неисправностей
А.10.10.6 Синхронизация часов

Контроль доступа (A.11)

A.11.1 Бизнес-требования к контролю доступа

Цель: Контролировать доступ к информации

A.11.1.1 Политика контроля доступа

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

A.11.2.2 Управление привилегиями

A.11.2.3 Управление паролями пользователей

A.11.2.4 Пересмотр прав доступа пользователей

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

A.11.3.2 Оборудование, оставленное пользователем без присмотра

A.11.3.3 Правила «чистого стола» и «чистого экрана»

A.11.4 Контроль сетевого доступа

Цель: Предотвратить несанкционированный доступ к сетевым сервисам

A.11.4.1 Политика в отношении использования сетевых услуг

A.11.4.2 Аутентификация пользователей для внешних соединений

A.11.4.3 Идентификация оборудования в сетях

A.11.4.4 Защита диагностических и конфигурационных портов при удаленном доступе

A.11.4.5 Принцип разделения в сетях

A.11.4.6 Контроль сетевых соединений

A.11.4.7 Контроль маршрутизации в сети

Контроль доступа (A.11)

A.11.5 Контроль доступа к операционной системе

Цель: Предотвратить несанкционированный доступ к операционным системам

A.11.5.1 Безопасные процедуры регистрации

A.11.5.2 Идентификация и аутентификация пользователя

A.11.5.3 Система управления паролями

A.11.5.4 Использование системных утилит

A.11.5.5 Периоды бездействия в сеансах связи

A.11.5.6 Ограничение времени соединения

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

A.11.6.2 Изоляция систем, обрабатывающих важную информацию

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

A.11.7.2 Работа в дистанционном режиме

Разработка, внедрение и обслуживание информационных систем (А.12)

А.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

А.12.1.1 Анализ и детализация требований безопасности

А.12.2 Правильная обработка данных в приложениях

Цель: Предотвратить ошибки, потерю, несанкционированную модификацию или неправильное использование информации в приложениях

А.12.2.1 Проверка достоверности входных данных

А.12.2.2 Контроль обработки данных в приложениях

А.12.2.3 Целостность сообщений

А.12.2.4 Подтверждение достоверности выходных данных

А.12.3 Криптографические средства защиты

Цель: Защищать конфиденциальность, аутентичность или целостность информации криптографическими средствами

А.12.3.1 Политика использования криптографических средств защиты

А.12.3.2 Управление ключами

А.12.4 Безопасность системных файлов

Цель: Обеспечить безопасность системных файлов

А.12.4.1 Контроль программного обеспечения, находящегося в промышленной эксплуатации

А.12.4.2 Защита данных тестирования системы

А.12.4.3 Контроль доступа к исходным кодам

А.12.5 Безопасность в процессах разработки и поддержки

Цель: Поддерживать безопасность программного обеспечения прикладных систем и содержащейся в них информации

А.12.5.1 Процедуры контроля изменений

А.12.5.2 Технический анализ прикладных систем после внесения изменений в операционные системы

А.12.5.3 Ограничения на внесение изменений в пакеты программ

А.12.5.4 Утечка информации

А.12.5.5 Разработка программного обеспечения с привлечением сторонних организаций

А.12.6 Менеджмент технических уязвимостей

Цель: Снизить риски, являющиеся результатом использования опубликованных технических уязвимостей

А.12.6.1 Управление техническими уязвимостями

Управление инцидентами информационной безопасности (A.13)

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

A.13.1.2 Оповещение о недостатках безопасности

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

A.13.2.2 Извлечение уроков из инцидентов информационной безопасности

A.13.2.3 Сбор доказательств

Управление непрерывностью бизнеса (A.14)

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

A.14.1.2 Непрерывность бизнеса и оценка риска

A.14.1.3 Разработка и внедрение планов непрерывности бизнеса, включающих в себя информационную безопасность

A.14.1.4 Структура плана обеспечения непрерывности бизнеса

A.14.1.5 Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса

Соответствие требованиям (A.15)

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
A.15.1.2 Права на интеллектуальную собственность
A.15.1.3 Защита учетных записей организации
A.15.1.4 Защита данных и конфиденциальность персональной информации
A.15.1.5 Предотвращение нецелевого использования средств обработки информации
A.15.1.6 Регулирование использования средств криптографической защиты

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
A.15.2.2 Проверка технического соответствия требованиям безопасности

Цель: Повышение эффективности процесса аудита информационных систем и снижение негативного влияния, связанного с данным процессом

A.15.3.1 Меры управления аудитом информационных систем
A.15.3.2 Защита инструментальных средств аудита информационных систем

Выводы

ГОСТ 27002 содержит более 800 рекомендаций по 10 разделам информационной безопасности. Каждый раздел представляет собой частную политику.