Академия ФСО России

Управление информационной безопасностью телекоммуникационных систем

Кафедра № 33

Тема 1. Система управления информационной безопасностью ТКС

Занятие 1. **Основы управления информационной безопасностью**

Учебные вопросы занятия:

1. Цели и задачи курса. Предмет, объект, структура и краткое содержание курса. Методические рекомендации по изучению курса.
2. Роль и место системы управления безопасностью в системе управления ТКС.
3. Система управления ИБ
4. Процесс управления ИБ

Литература

1. Управление информационной безопасностью телекоммуникационных систем : учебно-методическое пособие / А.Н. Цибуля и др.; под общ. ред. А.И. Козачка – Орёл : Академия ФСО России, 2018. – 248 с.
2. Системы анализа защищенности: практическое пособие / А.А. Юркин и др.; под общ ред. А.А. Юркина. – Орел : Академия ФСО России, 2017. – 140 с.
3. Системы анализа защищенности : пособие / А.И. Козачок [и др.] ; под общ. ред. А.И. Козачка. – Орёл : Академия ФСО России, 2014. – 131 с.
4. Управление информационной безопасностью : монография / [А. И. Козачок, В.В. Комашинский, А.А. Юркин и др.]. – Орёл : Академия ФСО России, 2013. – 328 с.
5. Курило, А.П., Милославская, Н.Г., Сенаторов, М.Ю., Толстой, А.И. Основы управления информационной безопасностью. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2012. – 244 с.
6. Милославская, Н.Г., Сенаторов, М.Ю., Толстой, А.И. Управление рисками информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2012. – 130 с.
7. Милославская, Н.Г., Сенаторов, М.Ю., Толстой, А.И. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2014. – 166 с.
8. Милославская, Н.Г., Сенаторов, М.Ю., Толстой, А.И. Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2012. – 214 с.
9. Милославская, Н.Г., Сенаторов, М.Ю., Толстой, А.И. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2014. – 170 с.
10. Основы построения и функционирования систем обнаружения и предупреждения компьютерных атак : учебно-методическое пособие / Д.Е. Шугуров, А.И. Козачок, П.Н. Горбачев и др. – Орел : Академия ФСО России, 2021. – 276 с.

Вопрос № 1

Цели и задачи курса. Предмет, объект, структура и краткое содержание курса. Методические рекомендации по изучению курса

Задачи дисциплины

- воспитание у курсантов активной жизненной позиции, научности мышления, творческого отношения к делу, любови к избранной профессии, чувства ответственности за достигнутые в обучении результаты;
- формирование знаний об особенностях архитектуры системы управления информационной безопасностью;
- формирование знаний и умений по управлению рисками, мониторинга, аудита и управления инцидентами информационной безопасности;
- формирование владения опытом работы с системами и средствами управления информационной безопасностью;
- формирование владения опытом администрирования и конфигурирования систем предупреждения и обнаружения атак;
- развитие способностей по использованию инструментальных средств для защиты от разрушающих программных средств, администрированию и конфигурированию программно-аппаратных средств защиты.

Требования к уровню освоения содержания дисциплины

знать:

- основные нормативные правовые акты в области управления информационной безопасностью, документы ФСТЭК России, а также международные нормативные методические документы в данной области (ОК-5, ПК-10, ПК-13, ПСК-33.2, ВПК-33.2, ВПК-33.3);
- модели, методы и средства управления информационной безопасностью (ПК-14, ПК-15, ПСК-33.2, ВПК-33.2, ВПК-33.3);
- принципы и методы функционирования систем обнаружения атак, порядок обнаружения компьютерных вторжений и сетевых атак (ПК-14, ПК-15, ПСК-33.2, ВПК-33.2, ВПК-33.3);

Требования к уровню освоения содержания дисциплины

уметь:

- формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе (ПК-10, ПСК-33.2, ВПК-33.2, ВПК-33.3);
- проводить анализ защищенности сетей специальной связи с использование инструментальных средств (ВПК-33.3);
- администрировать подсистемы аудита, мониторинга информационной безопасности и управления качеством обслуживания ТКС (ОПК-5, ПК-14, ПСК-33.2, ВПК-33.2, ВПК-33.3);
- идентифицировать и анализировать активы, угрозы и уязвимости объекта информатизации и оценивать риски информационной безопасности (ОПК-5, ПК-8, ПК-11, ПСК-33.2, ВПК-33.2, ВПК-33.3);
- обеспечивать защиту ПО от ВПО (ОПК-5, ПК-14, ПСК-33.2);
- анализировать программное обеспечение на наличие вирусов и программных закладок (ОПК-5, ПК-14, ПСК-33.2, ВПК-33.2, ВПК-33.3);

владеть:

- навыками работы с системами и средствами управления информационной безопасностью и качеством обслуживания ТКС (ОПК-5, ПК-14, ПСК-33.2, ВПК-33.2, ВПК-33.3);
- методами и средствами выявления угроз, уязвимостей, оценки рисков, оценки защищенности, аудита и мониторинга информационной безопасности (ОПК-5, ПК-8, ПК-11, ПК-14, ПСК-33.2, ВПК-33.2, ВПК-33.3);
- навыками защиты от ВПО и компьютерных атак (ОПК-5, ПК-8, ПК-11, ПК-14, ПСК-33.2, ВПК-33.2, ВПК-33.3).

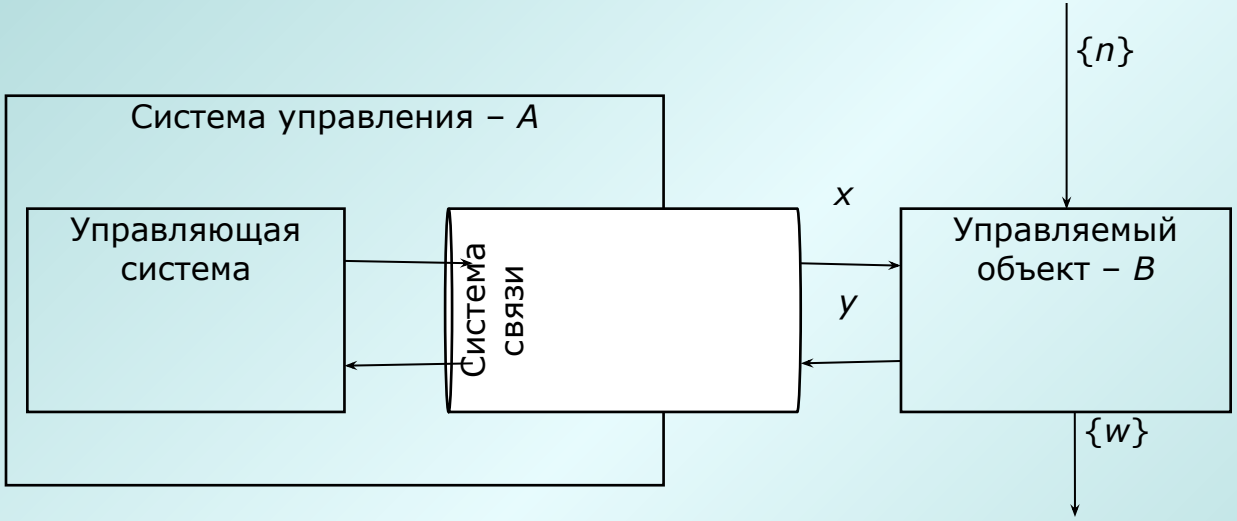
Распределение времени изучения дисциплины по темам

Наименование разделов и тем	К-во часов аудит. занят.	Кол-во часов СР	Распределение времени по видам занятий						Количество и виды текущего, промежуточного и итогового контроля			
			Лек.	Гр. зан.	Пр. зан.	СРРП	С	Экз	ДКЗ	РГР	КП	Экз
8 семестр												
Тема 1. **Система управления ИБ ТКС**	12	12	2	6	4							
Тема 2. **Управление защищенностью ТКС**	18	20		4	16					1		
Тема 3. **Системы обнаружения и предупреждения атак**	24	24	2	8	14							
Тема 4. **Защита от вредоносного ПО**	16	16	2	6	6		2					
Тема 5. **Управление инцидентами ИБ**	20	18		6	8	2	2				1	
Экзамен	18+6	9						6				1
Всего за дисциплину	114	102	6	28	26	8	4	6		1	1	1

Вопрос № 2

Роль и место системы управления безопасностью в системе управления ТКС

Система с управлением



{*x*} - входная информация;
{*u*} ⊆ {*x*} - командная информация;
{*y*} - выходная информация;
{*n*} - воздействие окружающей среды (помехи);
{*w*} - показатели, характеризующие качество и эффективность функционирования УО.

Функции управления

Основные функции системы управления на каждом уровне ЭМВОС:
Управление сбоями/событиями (Fault management).
Управление конфигурациями (Configuration Management).
Управление статистической информацией.
Управление производительностью.
Управление безопасностью (Security management):

- контроль конфигурацией;
- управление потоками данных;
- мониторинг производительности;
- управление отказами;
- управление информационной безопасностью:

Управление:

✔ политикой безопасности (ПБ);
✔ архитектурой системы защиты информации (СЗИ);
✔ механизмами защиты;
✔ средствами защиты.

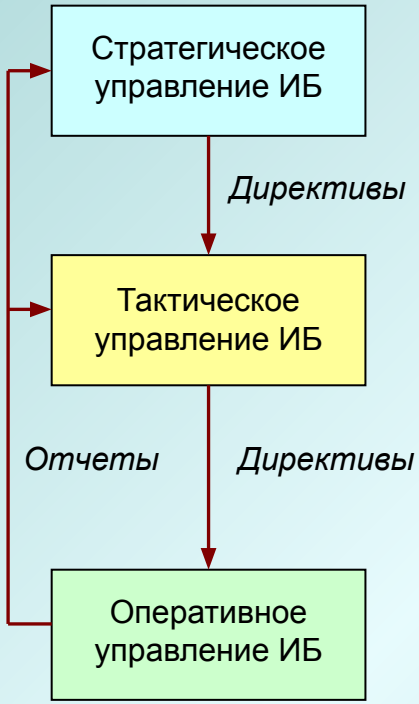
Задачи управления ИБ

В ходе управления ИБ решаются следующие задачи:

- разграничение доступа к ресурсам;
- настройка функций служб сетевых устройств;
- ведение журналов регистрации событий;
- генерация отчетов о событиях, относящихся к безопасности;
- обеспечение конфиденциальности данных;
- авторизация прав доступа у пользователей;
- выявление уязвимостей и попыток НСД;
- распространение конфигурационных настроек безопасности на элементы сети;
- обучение и информирование пользователей по вопросам ИБ.

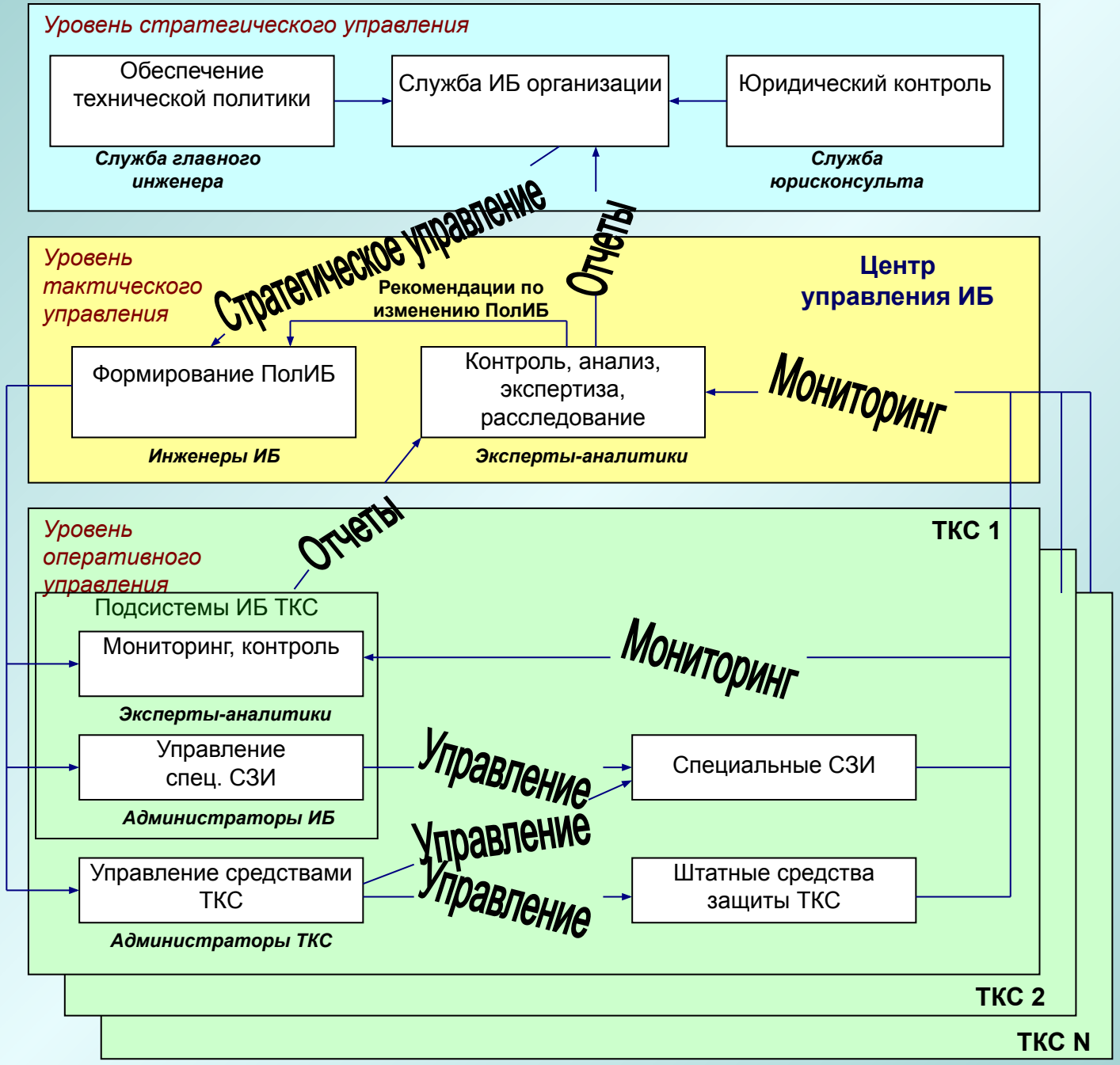
Управление ИБ заключается в четком выполнении всех задач по планированию, реализации, проверке и совершенствованию СЗИ с требуемым качеством, нацеленных на недопущение реализации угроз, атак и деструктивных воздействий на информацию, а также по их локализации, минимизации ущерба.

Уровни управления ИБ организации



Назначение	*Основные задачи*
Обеспечение интересов организации в области ИБ	**Определение стратегии и разработка концепции ИБ. Основные направления ОИБ. Нормативно-правовое ОИБ.**
Формирование и контроль выполнения ПолИБ	**Планирование и обеспечение выполнения ПолИБ. Разработка положений, регламентов, правил, инструкций. Проведение расследований и анализ инцидентов ИБ.**
Реализация выполнения требований ПолИБ	**Обеспечение механизмов и способов ОИБ. Реализация защитных функций и процедур. Эксплуатация средств защиты и контроля.**

Функциональная структура управления ИБ организации



Виды управления ИБ

Организационное управление – планирование, управление проектами по ИБ и персоналом.

Программно-техническое управление – управление инженерно-технической и программно-аппаратной ЗИ.

Юридическое управление – формирование методических рекомендаций, ПБ и нормативно-правовых актов по ИБ.

Организационное управление ИБ подразделяется на управление:

- рисками;
- отчетами (оценка и анализ защищенности);
- проектами (проектированием СЗИ и СУИБ);
- специальными работами (специсследованиями и спецпроверками технических средств; аттестованием объектов и помещений; экспертизой, лицензированием и сертификацией СЗИ);
- документами (ключевыми документами, заявками на проведение специальных работ, техническим обслуживанием и ремонтом);
- инцидентами (определение инцидента, оповещение о его возникновении, регистрация инцидента, устранение его последствий и причин, расследование инцидента, реализация действий, предупреждающих повторное его возникновение);
- подразделением ИБ и персоналом организации (изучение, инструктирование, обучение и контроль).

Основными видами программно-технического управления ИБ являются управление:

- уязвимостями (на этапе проверки и непосредственного ввода в эксплуатацию или текущего контроля перед возобновлением работы в период функционирования);
- угрозами (предотвращением воздействий в период основного функционирования; отражением компьютерных атак, вредоносного программного обеспечения (ПО) и утечкой по портам);
- мониторингом безопасности (в том числе и радиотехническим), наличия (инвентаризации) и функционирования (производительности);
- приложениями и обновлениями ПО по ИБ.

Важными видами юридического управления ИБ являются:

- формирование общих требований, заданий по ИБ и специальных технических требований по защите информации;
- составление ПБ и договоров на ограничения;
- выработка методик и методических рекомендаций по соблюдению правил ИБ;
- издание приказов и распоряжений, ведомственных нормативно-правовых актов по ИБ.

Взаимосвязь СОИБ с технологическими системами СЭСв ОП

Вопрос № 3

Система управления ИБ

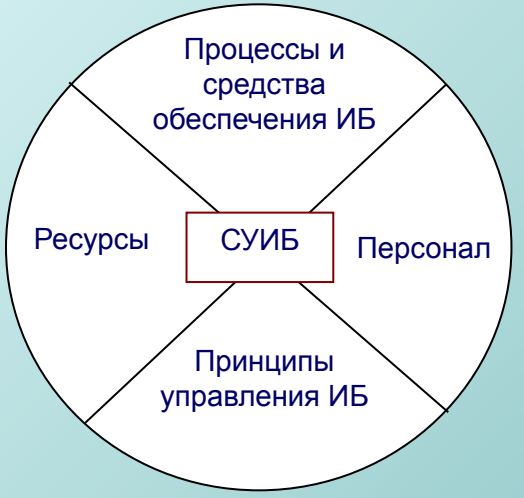
СУИБ *(англ.* information security management system) - часть общей системы управления организации, основанную на подходе оценки и анализа бизнес-рисков, предназначенную для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения *ИБ,* и включающую организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области ИБ.

Функции СУИБ:

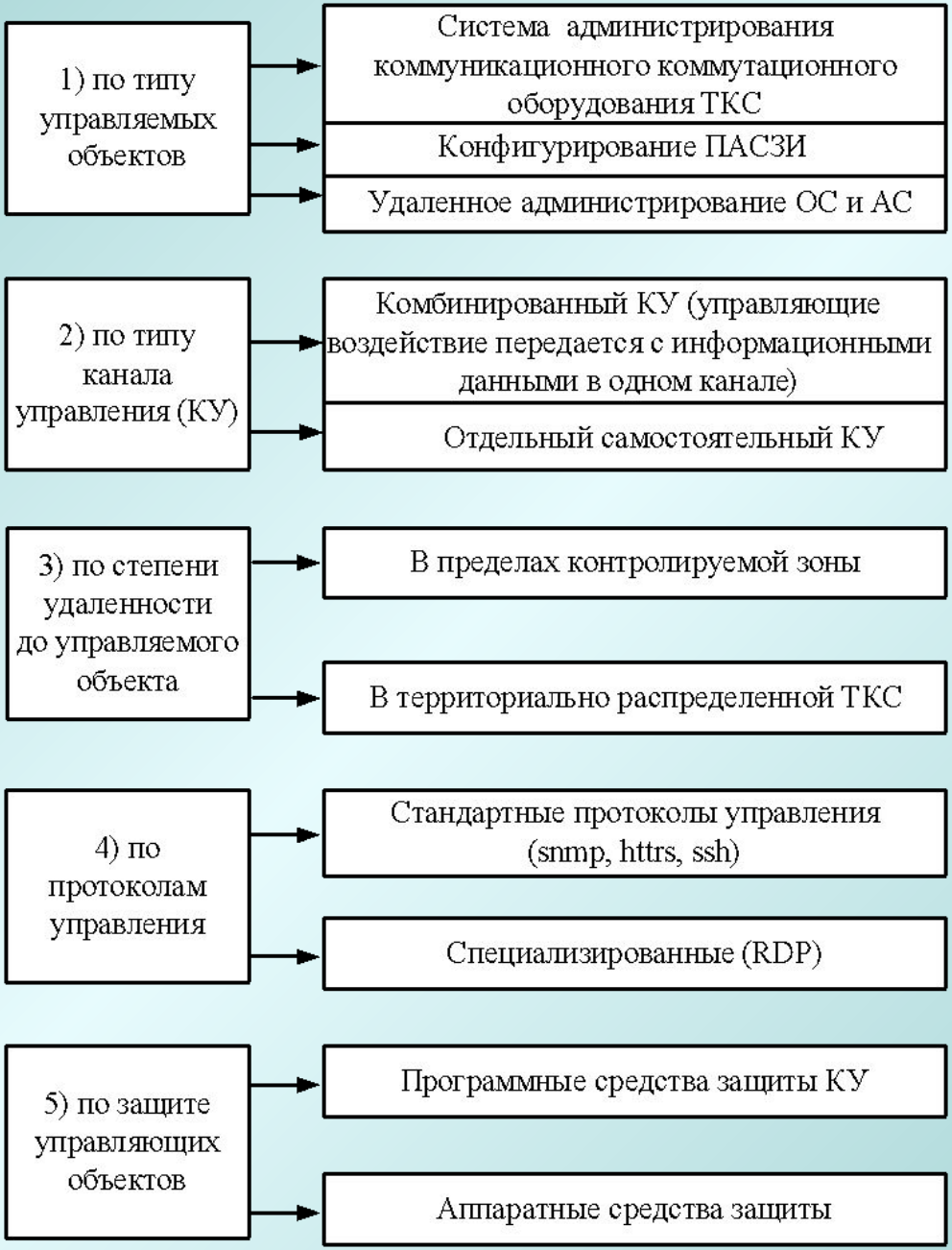
- ✔ реализация целенаправленного, систематического и комплексного подхода к управлению ИБ защищаемых активов, что приводит к повышению текущего уровня их защищенности;
- ✔ объединение всех применяемых в организации защитных и организационных меры в единый, адекватный реальным угрозам ИБ и управляемый комплекс, позволяющий достигать целей ОИБ на уровне всей организации;
- ✔ позволяет четко установить, как взаимосвязаны процессы и подсистемы ОИБ, кто за них отвечает, какие финансовые и трудовые ресурсы необходимы для их эффективного функционирования и т. д.;
- ✔ проводит процесс выполнения ПолИБ и позволяет находить и устранять слабые места в ОИБ;
- ✔ охватывает людей, процессы и ИТ-структуру организации.

Компоненты СУИБ

1. Соответствующая организационная структура с поддерживающими ее подсистемами автоматизации функционирования СУИБ (документооборотом, обработкой, хранением и передачей данных и т. п.), организации управления и собственной защиты;
2. Модель функционирования СУИБ (например, процессно-ролевая);
3. Методики и методы управления ИБ (методика управления ИБ – общий свод правил, алгоритм, приемы управления ИБ; метод управления ИБ – путь практического осуществления деятельности по управлению ИБ, способ достижения определенной цели в рамках ОИБ);
4. Документальное обеспечение функционирования СУИБ – Политика СУИБ, планы СУИБ, процедуры, регламенты и т. д.;
5. Деятельность по планированию, реализации, проверке и совершенствованию СУИБ с соответствующими средствами выполнения конкретной деятельности;
6. Ответственность всех участвующих в процессе управления ИБ, и тех, кто попадает в область действия СУИБ;
7. Процессы управления ИБ, выполняемые на основе СУИБ;
8. Средства управления ИБ;
9. Необходимые ресурсы.

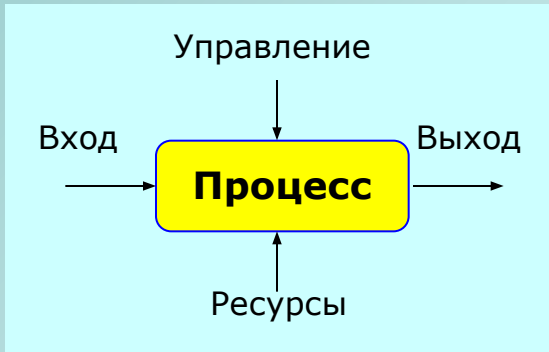


Классификация систем управления ИБ



Вопрос № 4

Процесс управления информационной безопасностью



ICOM-коды организации процесса

Процессы организации можно разделить на несколько основных групп:

Основные (процессы жизненного цикла), обеспечивающие намеченный результат деятельности организации. Назначение процесса - создание основных продуктов деятельности организации; результат - основной продукт и/или полуфабрикат для его изготовления для промежуточных процессов.

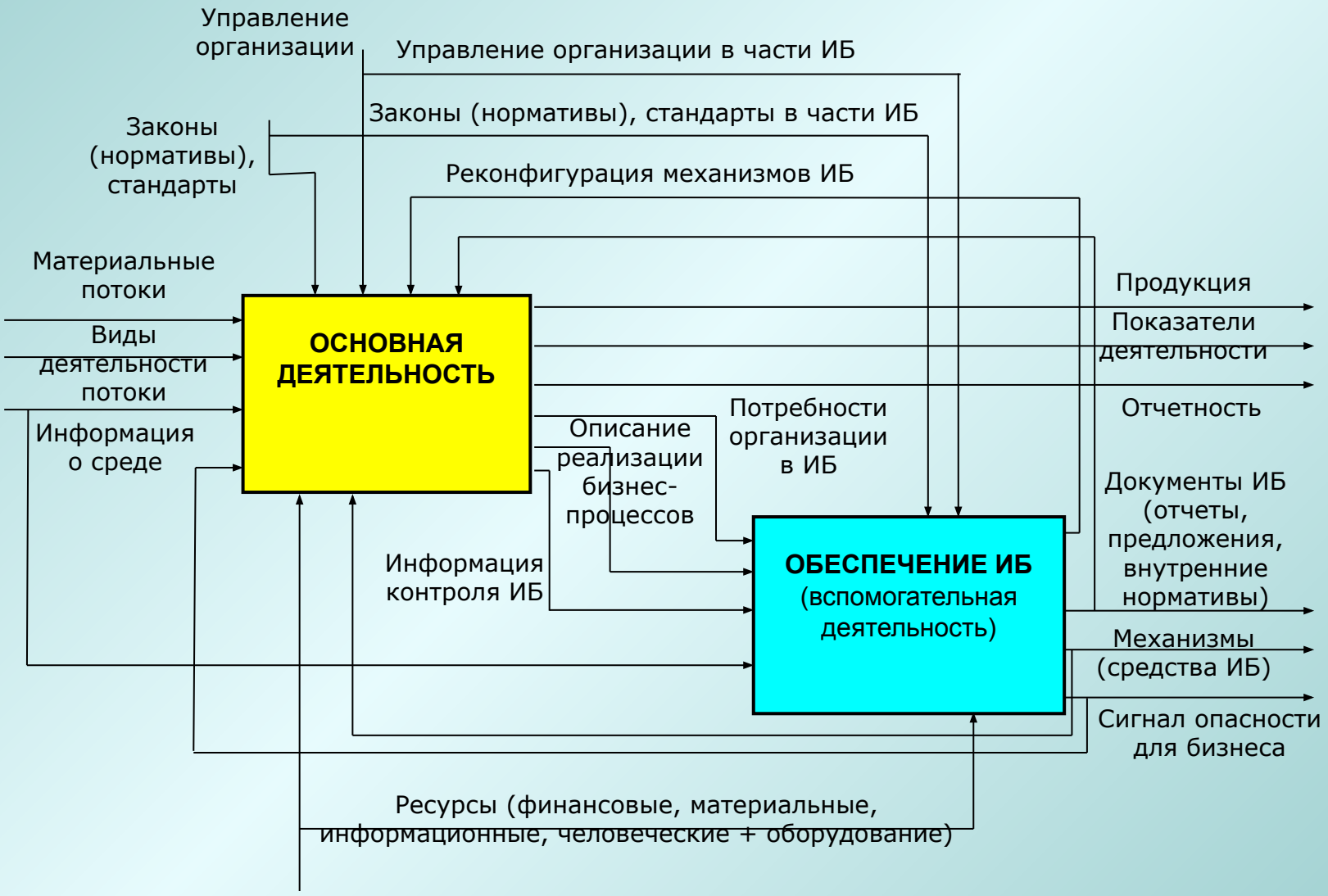
Вспомогательные, предназначенные для обеспечения нормального функционирования основных и других процессов необходимыми ресурсами; они обеспечивают работу основных (сервисное обслуживание оборудования, обеспечение энергоресурсами и производственной средой, обеспечение работы офиса, информационное обеспечение, обеспечение финансовой поддержки, управление окружающей средой, PR-деятельность и связь с общественностью и т. д.). Назначение процесса - обеспечение деятельности основных процессов; результат - ресурсы и сервисы для основных процессов. ОИБ относится к вспомогательной деятельности.

Процессы управления (менеджмента), относящиеся к стратегическому планированию, постановке целей и установлению политик, обеспечению коммуникаций и т. п. Назначение процесса - управление деятельностью организации; результат - деятельность всей организации. По своей природе управленческие задачи являются информационными.

Процессы измерения, анализа и совершенствования. Назначение процесса - входные данные для процессов усовершенствования всей деятельности организации; результат - совершенствование всей деятельности организации.

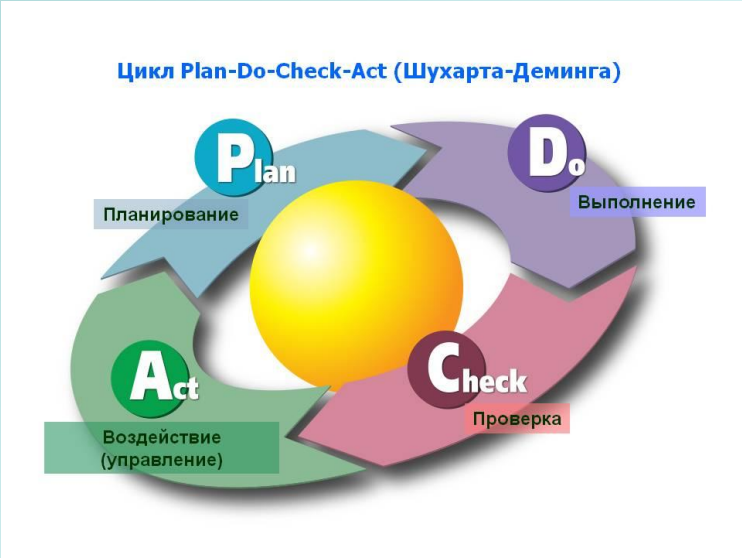
Бизнес-процесс *- множество из одной или нескольких упорядоченных во времени, логически связанных и завершенных видов деятельности, в совокупности поддерживающих деятельность организации и реализующих ее политику, направленную на достижение поставленных целей*.

Связи основной деятельности и деятельности по ОИБ организации



Модель PDCA

Процесс управления информационной безопасностью — это циклический набор действий, включающий:



- ✔ осознание степени необходимости защиты информации и постановку задач;
- ✔ сбор и анализ данных о состоянии информационной безопасности в организации;
- ✔ оценку информационных рисков;
- ✔ планирование мер по обработке рисков;
- ✔ реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий;
- ✔ мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия.

Основные процессы модели PDCA СУИБ

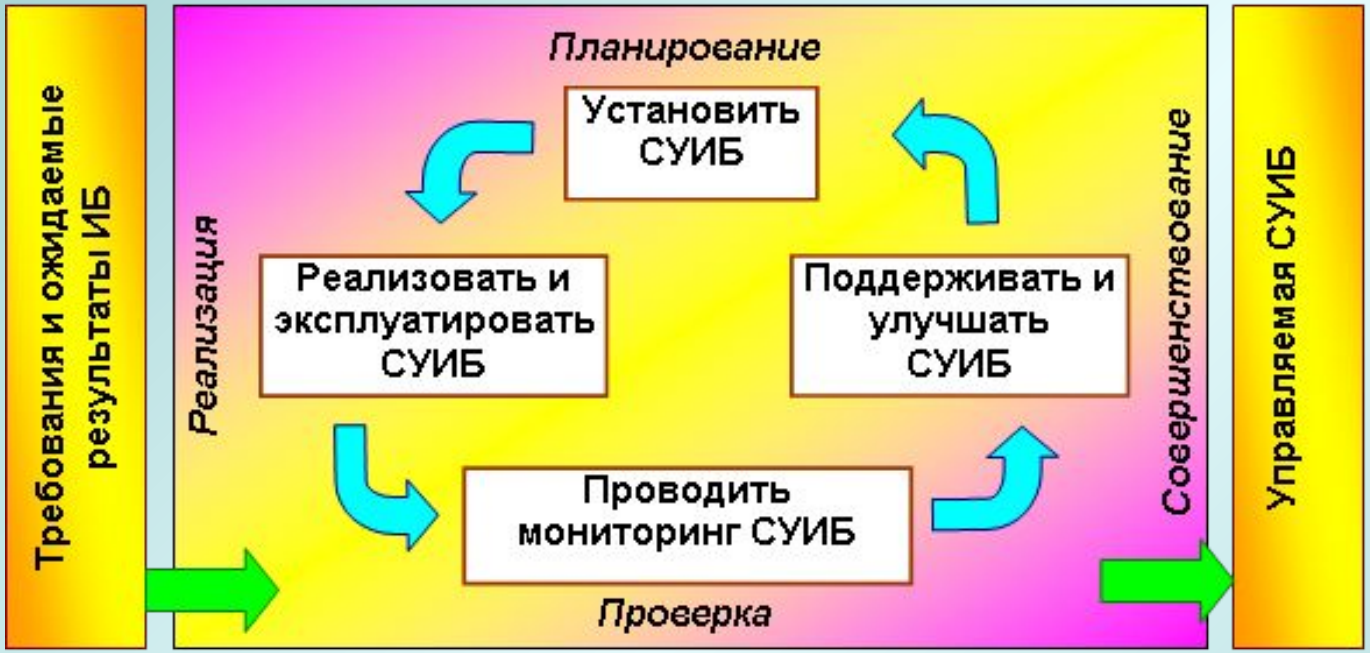


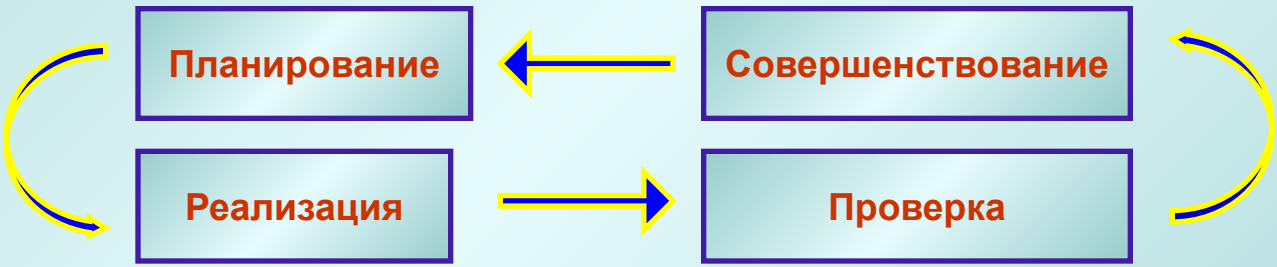
Таблица 1

Планирование (разработка СУИБ)	Определение политики СУИБ, целей, процессов и процедур, значимых для управления рисками и повышения информационной безопасности, с целью получения результатов, соответствующих общим политикам и целям организации.
Реализация (внедрение и эксплуатация СУИБ)	Реализация и использование политики СУИБ, средств управления, процессов и процедур.
Проверка (мониторинг и анализ СУИБ)	Оценка и, если требуется, измерение характеристик процесса для проверки соответствия политике СУИБ, целям и практическому опыту, а также передача результатов для последующего анализа управленческим персоналом.
Совершенствование (сопровождение и совершенствование СУИБ)	Принятие корректирующих и превентивных мер по результатам внутреннего аудита СУИБ и анализа, выполненного управленческим персоналом, а также на основе другой значимой информации, с целью постоянного совершенствования СУИБ.

Детализация процессов модели PDCA СУИБ

П1.1. Область и границы действия СУИБ
П1.2. Политика для СУИБ
П1.3. Подход к оценке рисков ИБ
П1.4. Идентификация рисков ИБ
П1.5. Оценка рисков ИБ
П1.6. Варианты обработки рисков ИБ
П1.7. Меры управления для обработки рисков ИБ
П1.8. Остаточные риски ИБ
П1.9. Разрешение на внедрение и эксплуатацию СУИБ
П1.10. Положение о применимости

С4.1. Тактические и стратегические улучшения СУИБ
С4.2. Корректирующие и предупреждающие действия
С4.3. Информирование о действиях/результатах по улучшению СУИБ заинтересованных сторон
С4.4. Обеспечение внедрения улучшений СУИБ



Р2.1. План обработки рисков
Р2.2. Меры управления
Р2.3. Измерение результативности выбранных мер управления
Р2. 4. Программы по обучению и повышению квалификации сотрудников
Р2.5. Управление работой СУИБ
Р2.6. Управление ресурсами СУИБ
Р2.7. Обнаружение событий ИБ и реагирование на инциденты ИБ
Р2.8. Обеспечение непрерывности бизнеса

П3.1. Мониторинг и анализ
П3.2. Регулярный анализ результативности СУИБ
П3.3. Измерение результативности мер управления
П3.4. Пересмотр оценки рисков
П3.4. Пересмотр оценки рисков
П3.5. Внутренние аудиты СУИБ
П3.6. Анализ СУИБ со стороны руководства
П3.7. Обновление планов ИБ
П3.8. Регистрация действий и событий, влияющих на СУИБ

Основные процессы СУИБ