ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Введение. Основные принципы построения защищенных систем

АКТУАЛЬНОСТЬ

По данным компании «Код безопасности» (securitycode.ru):

•ИБ-специалисты каждой второй компании обеспокоены атаками на рабочие станции с использованием внешнего носителя в обход внешнего периметра сети.

•В среднем российские компании используют решения трех вендоров для обеспечения сетевой безопасности.

• У половины российских компаний нет подразделения, отвечающего за сетевую безопасность.

•Удаленный доступ к информационным системам с помощью ноутбуков, планшетов и смартфонов используют 44% крупных компаний.

•Менее чем у четверти российских компаний внедрена централизованная система мониторинга ИБ (SIEM).

•На защиту корпоративных сетей компании в среднем выделяют 11% из ИТ-бюджета.

•Для оптимизации затрат на построение системы защиты, организации стремятся снизить уровень классификации информационных систем.

•Для 76% российских компаний важен вопрос обучения персонала, отвечающего за информационную безопасность.

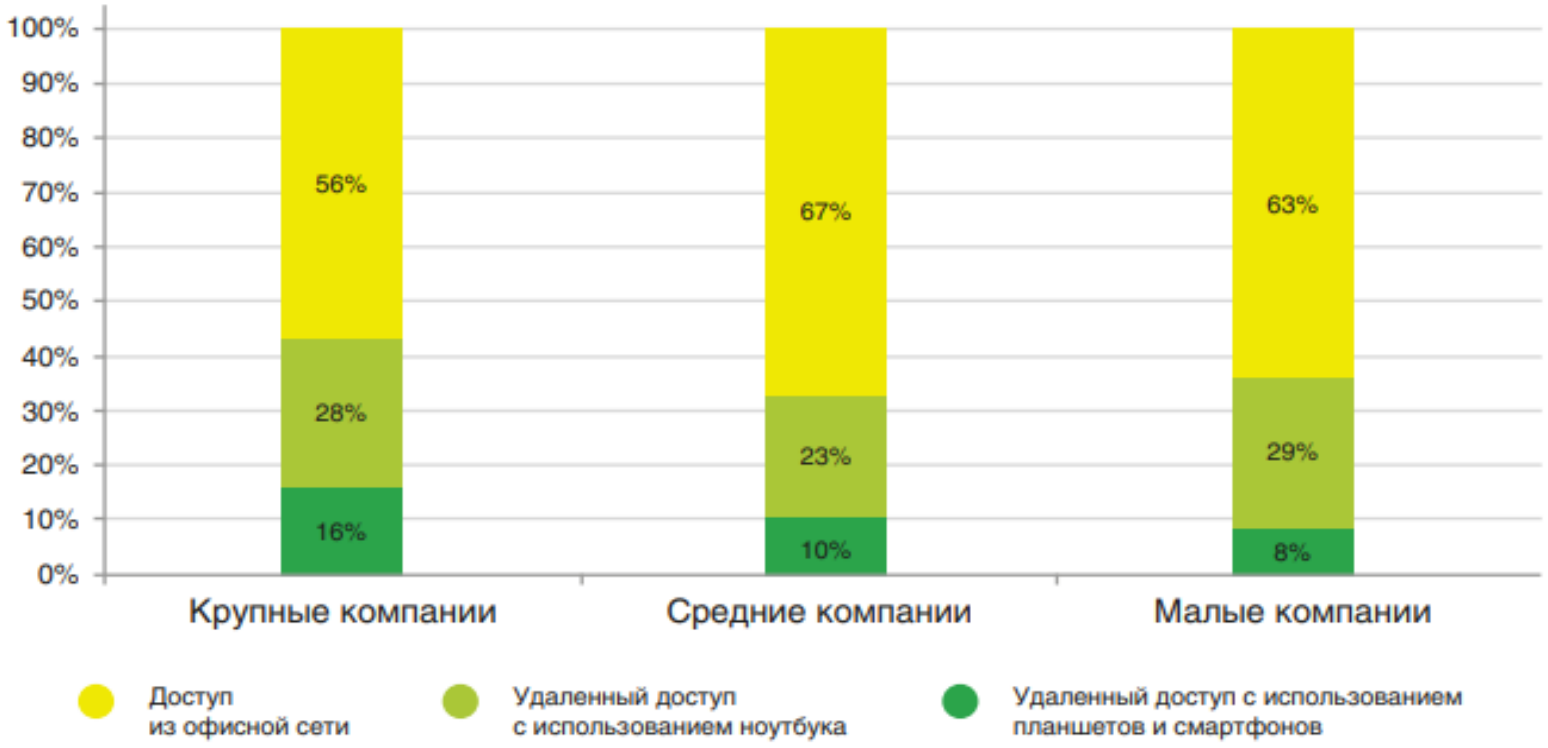
АКТУАЛЬНОСТЬ

- Возрастающая сложность программного и сетевого обеспечения, обеспечивающего взаимодействие на всех уровнях, приводит к:
- ошибкам в программном обеспечении, допущенным разработчиком
- ошибкам в настройке сетевого и программного обеспечения
- недостаточной идентификации и аутентификации удаленных компонентов компьютерной сети.

АКТУАЛЬНОСТЬ

КОД БЕЗОПАСНОСТИ

Организация доступа к ИС



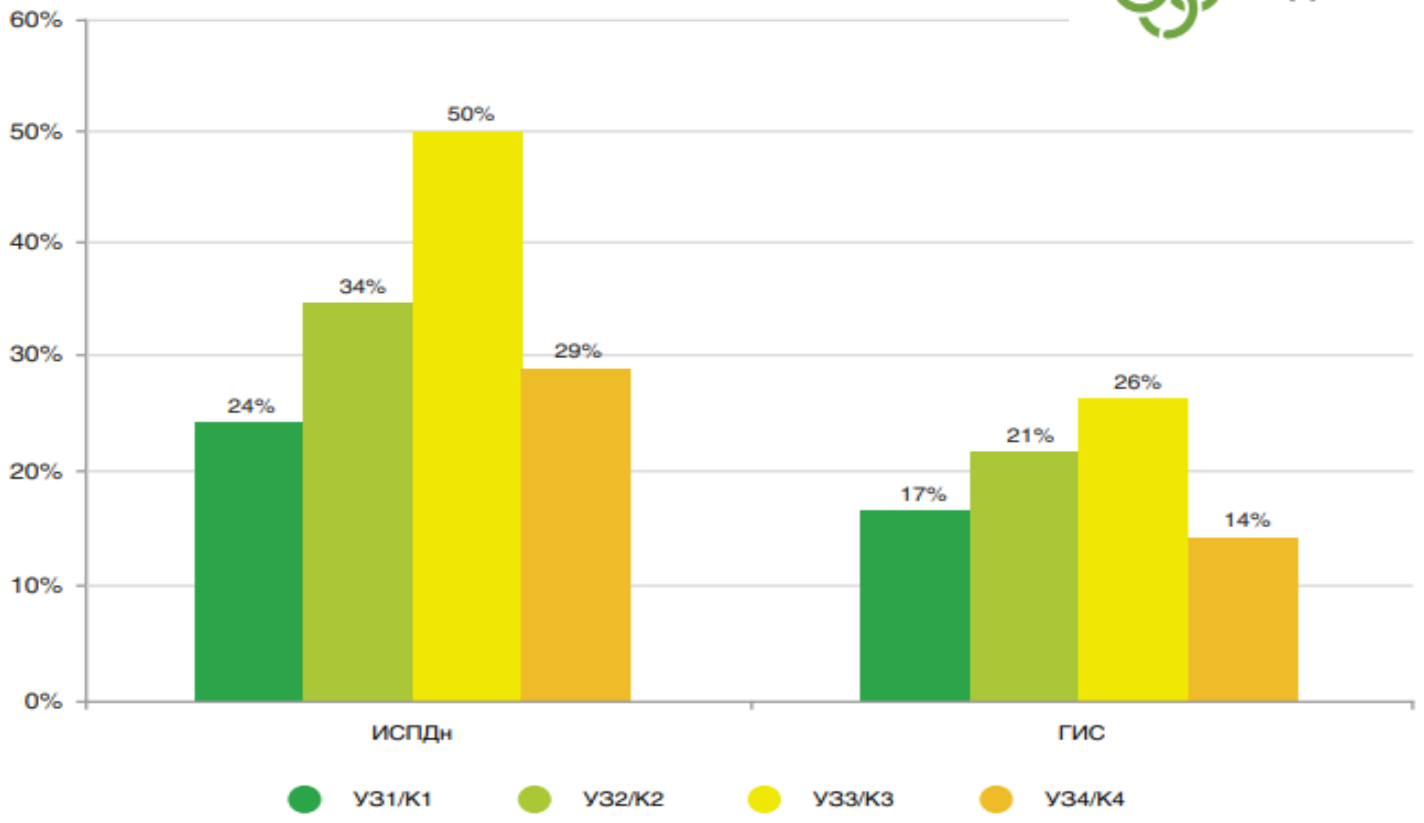
44% крупных компаний используют удаленный доступ к информационным системам с помощью ноутбуков, планшетов и смартфонов. В средних и малых компаниях наибольшие доли – 67% и 63% соответственно – приходятся на доступ из офисной сети.

АКТУАЛЬНОСТЬ

Для оптимизации затрат на построение системы защиты организации стремятся при классификации информационных систем минимизировать их класс.

Распределение классов информационных систем

КОД БЕЗОПАСНОСТИ



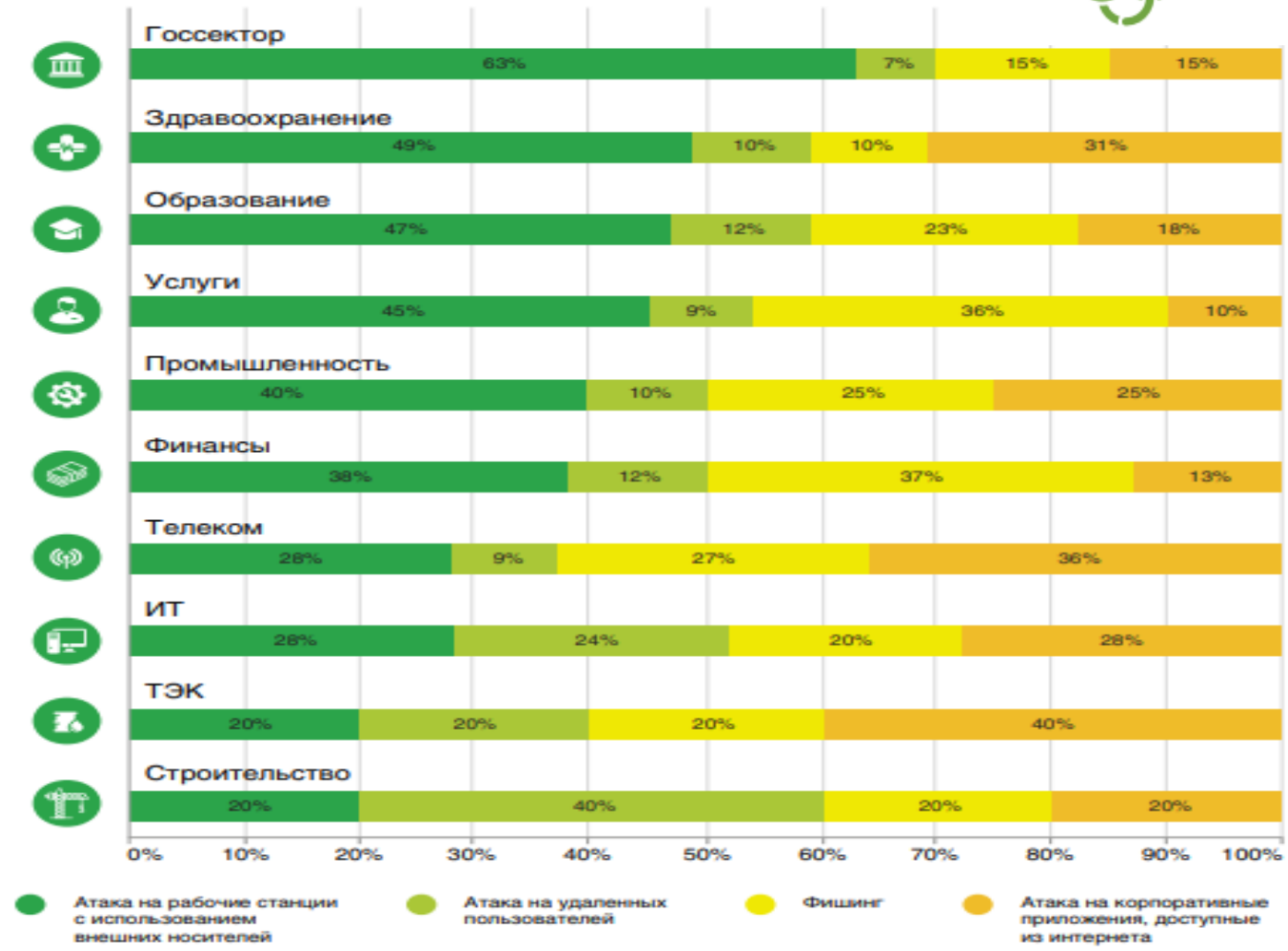
50% российских компаний используют информационную систему персональных данных по уровню защищенности УЗ3; 26% российских компаний обрабатывают информацию в ГИС по классу К3.

АКТУАЛЬНОСТЬ

По данным опроса, наибольшую опасность для информации корпоративной сети представляет атака на рабочие станции с использованием внешних носителей. Данную угрозу отметили 47% респондентов.

Актуальные способы проникновения в сеть

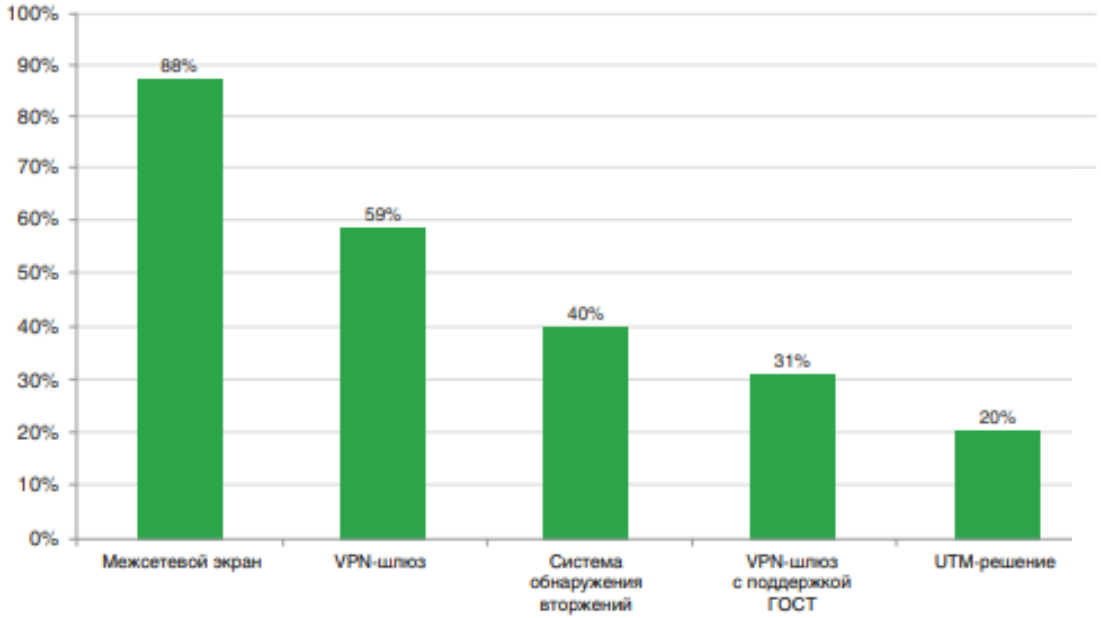
АКТУАЛЬНОСТЬ



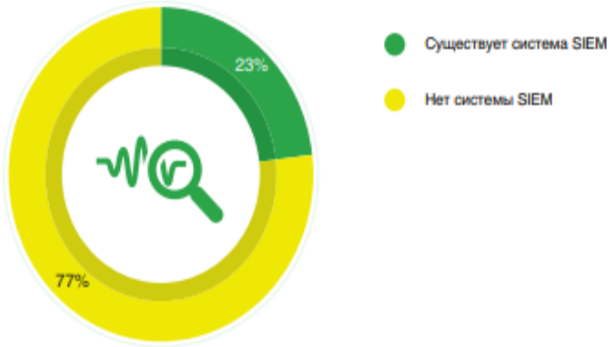
АКТУАЛЬНОСТЬ

КОД БЕЗОПАСНОСТИ

Какие СЗИ развернуты в структуре российских компаний



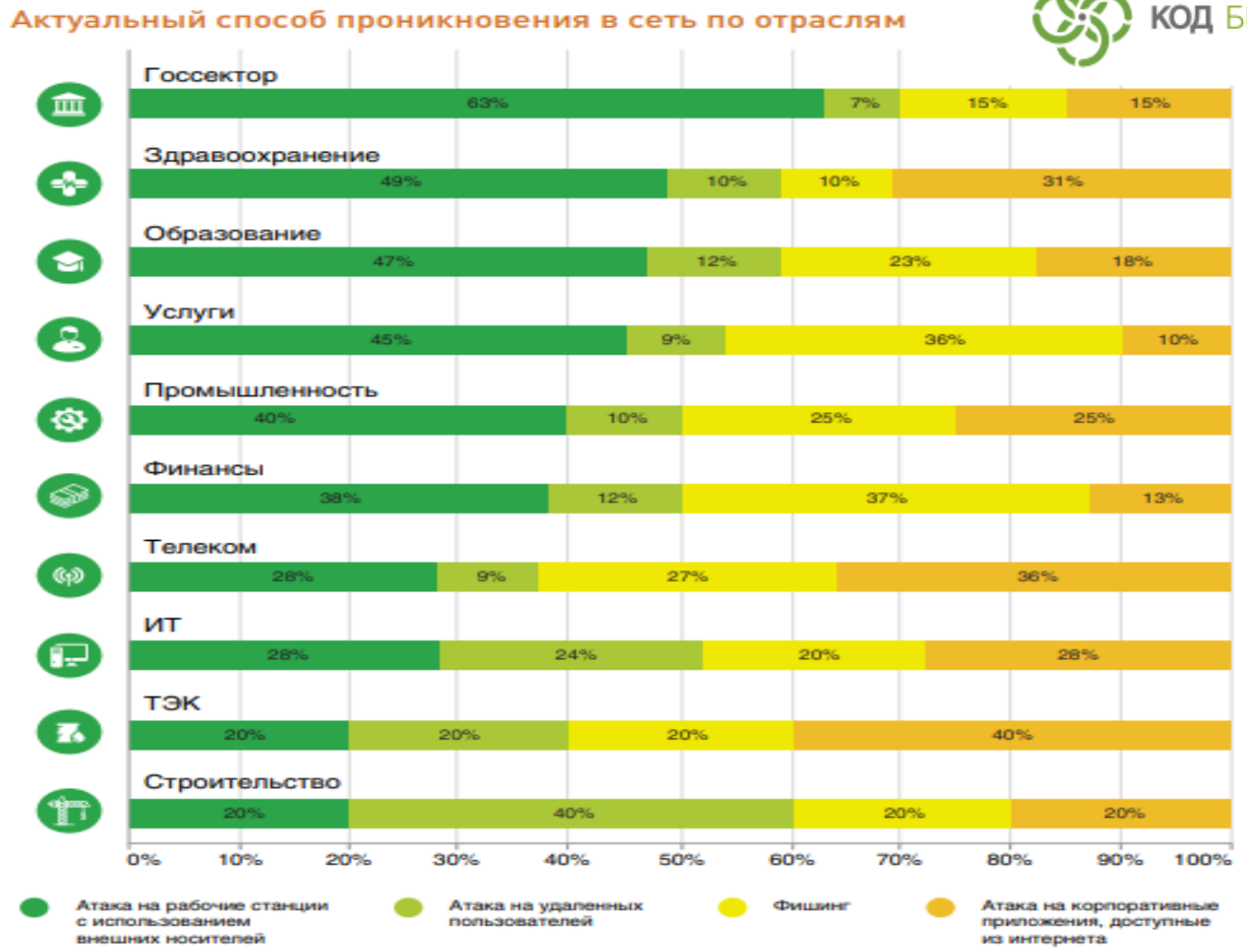
Наличие SIEM у российских компаний



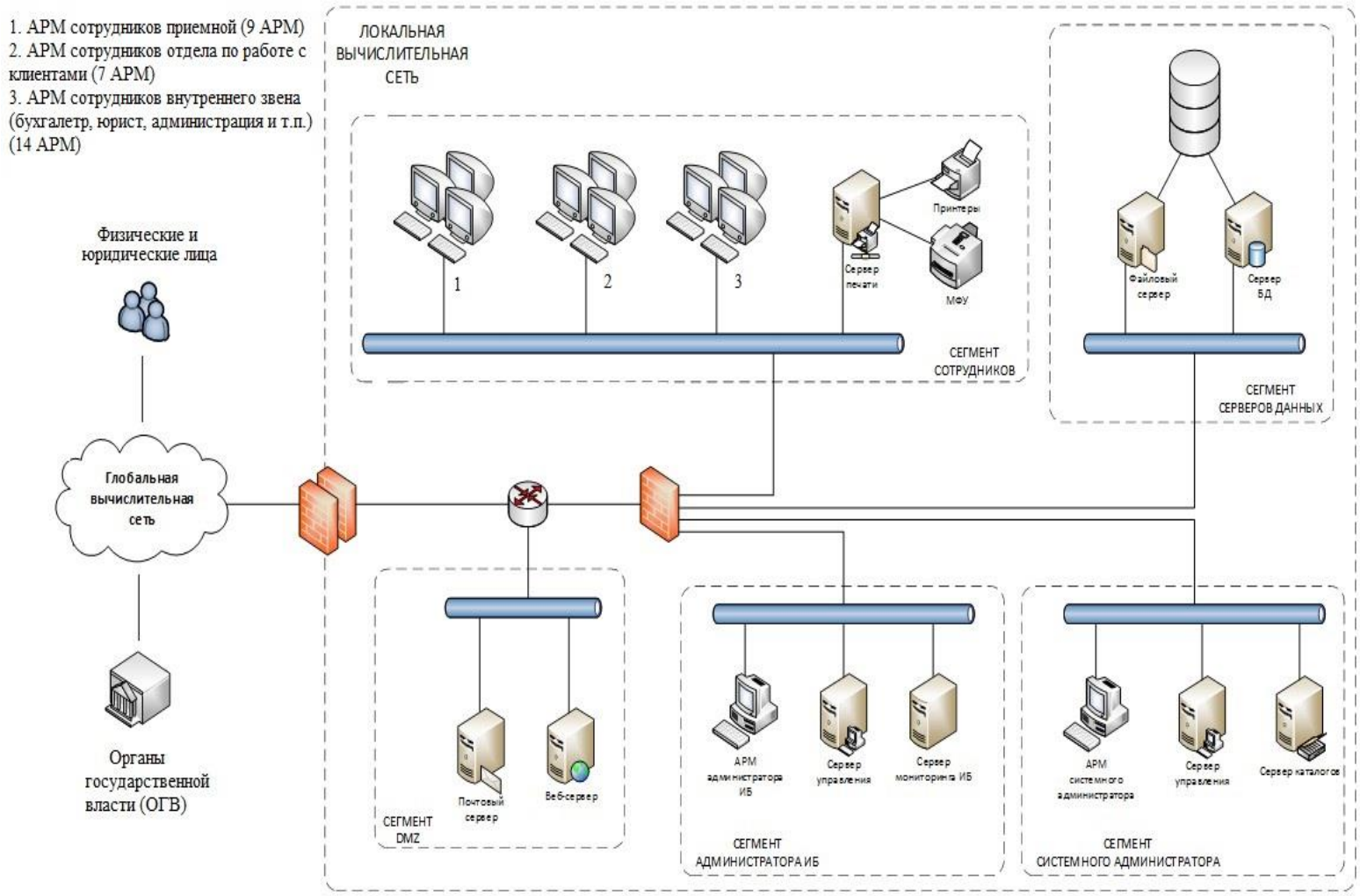
Межсетевой экран стоит у 88% участников опроса. VPN-шлюз есть у 59% респондентов. Данная защита востребована в топливно-энергетическом комплексе (60% компаний) и финансовом секторе (56% компаний). Система обнаружения вторжений востребована у половины организаций здравоохранения и информационных технологий. UTM-решение используют 20% российских компаний.

АКТУАЛЬНОСТЬ

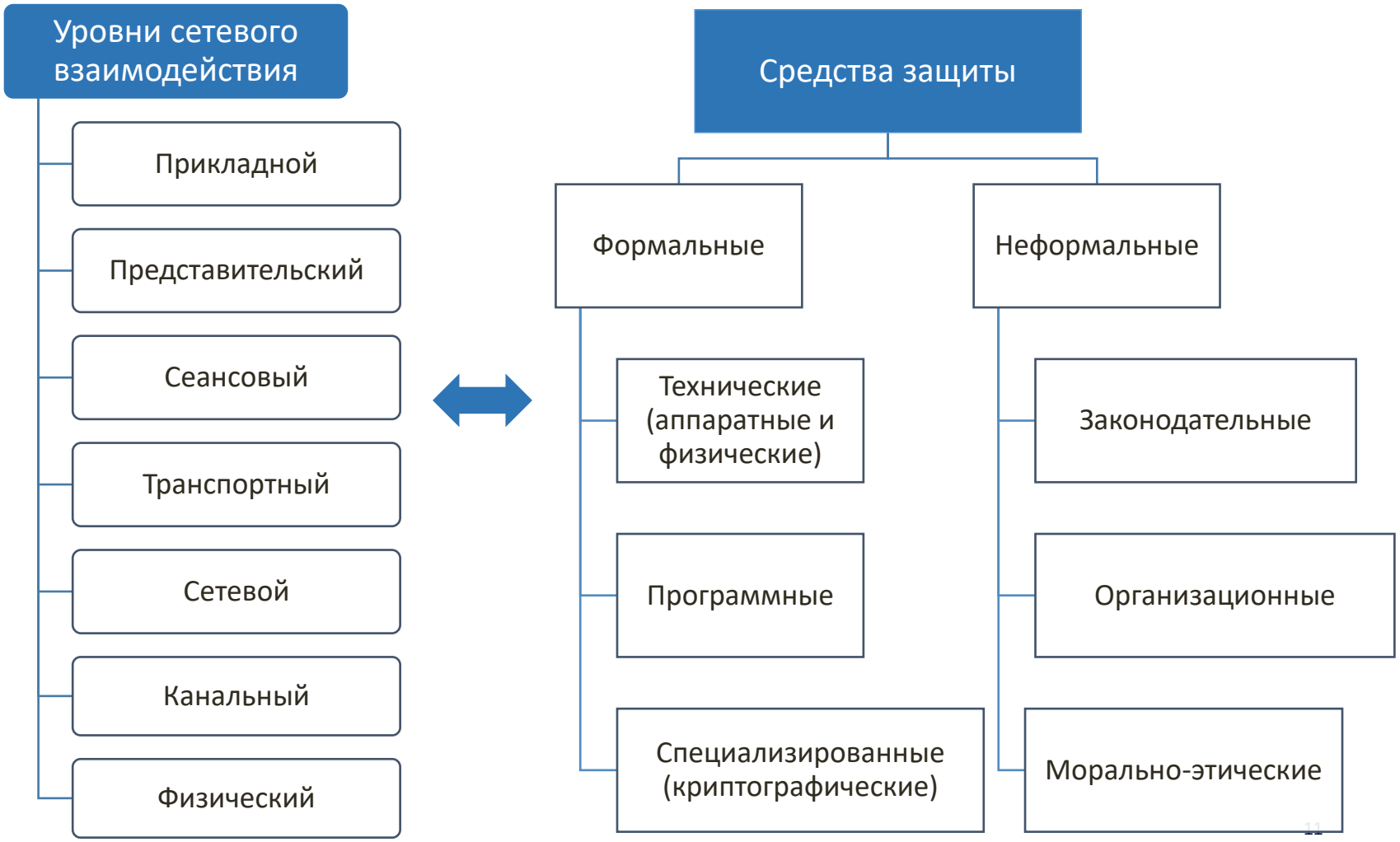
КОД БЕЗОПАСНОСТИ



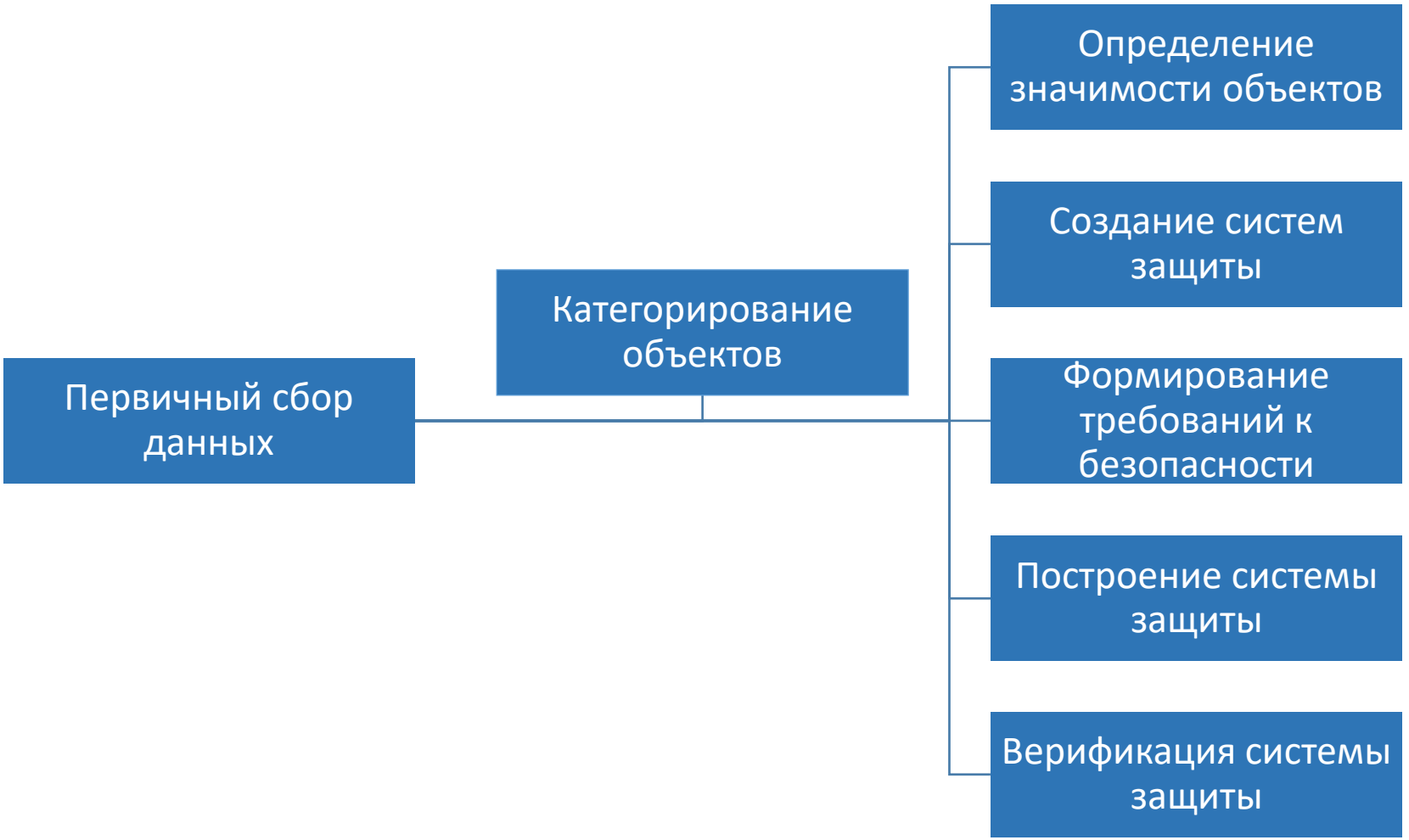
Основные элементы многоуровневой системы обеспечения защиты при передаче информации по каналам связи



Многоуровневая система обеспечения защиты при передаче информации по каналам связи



Основные принципы построения защищенных систем



Первичный сбор данных

Этап 1. Категорирование сферы в которой осуществляется циркуляция информации (определение сферы функционирования организации):

•Устав организации

• Положение об организации, Единый государственный реестр юридических лиц (ЕГРЮЛ)

•Единый государственный реестр индивидуальных предпринимателей (ЕГРИП)

•Лицензии и иные разрешительные документы на осуществление конкретных видов деятельности (выполнение работ, оказание услуг).

•Общероссийский классификатор видов экономической деятельности (ОКВЭД)

Пример

	Наименование ИС	ОКВЭД	Критичность объекта
1	Бухгалтерия	69.20.2	+
2	Отдел кадров	52.10.9	-
3	Производство	24.10.1	+

Первичный сбор данных

Этап 2. Категорирование ИС в которой осуществляется циркуляция информации (определения сферы функционирования организации):

•Следует учитывать, что для конкретной сферы будет преобладать один вид объекта, поскольку с большей вероятностью именно он будет обрабатывать информацию, необходимую для обеспечения критических процессов, и (или) осуществлять управление, контроль или мониторинг критических процессов.

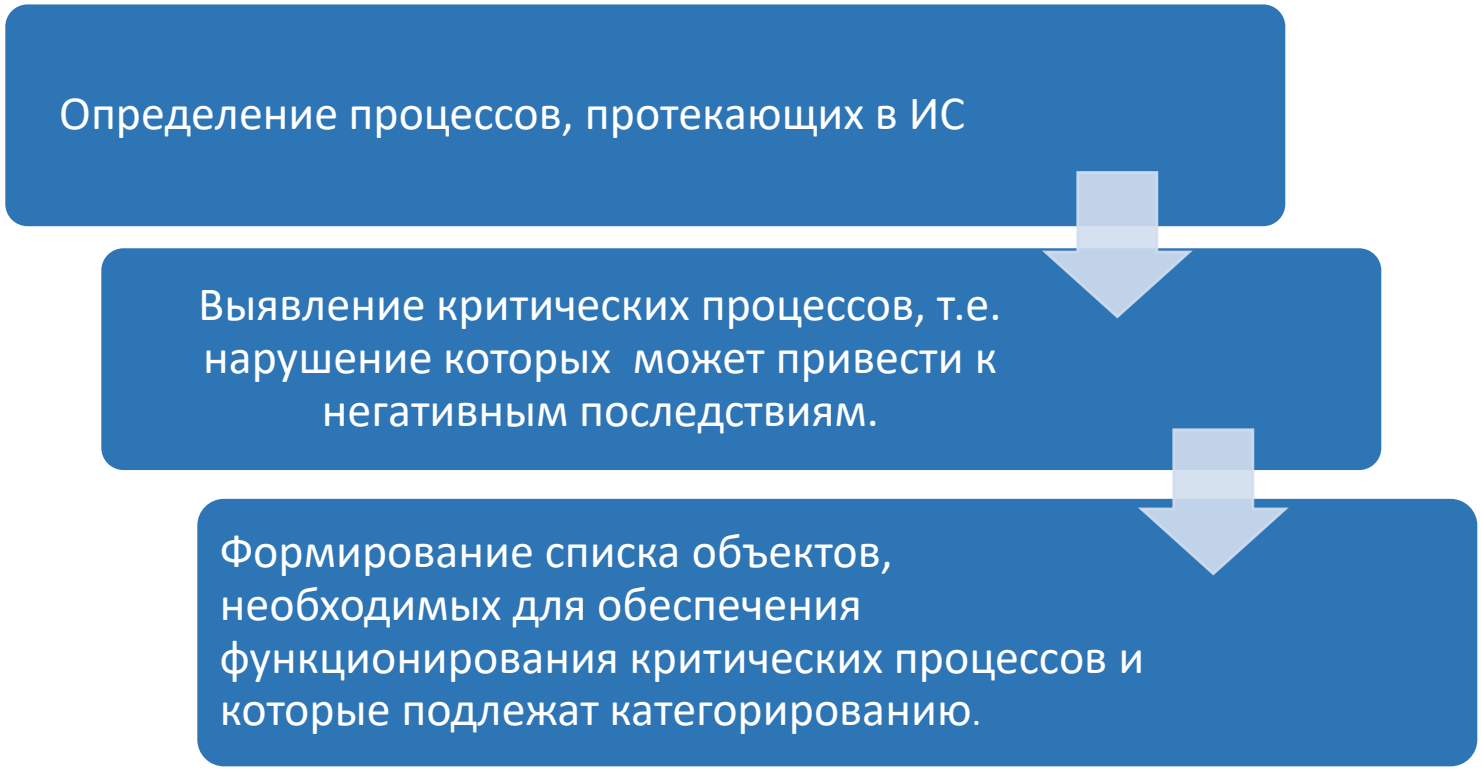
•Пример классификации объектов КИИ по сфере функционирования.

Пример

ИС	АСУ	ИТКС
Здравоохранение	Топливно-энергетический комплекс Энергетика	связь
Наука Транспорт	Атомная энергетика	
Банковская сфера	Ракетно-космическая промышленность	

Категорирование объектов. Определение значимости

Категорирование – установление соответствия объекта инфраструктуры критериям значимости и показателям их значений, на основании которых определяется базовый набор степени защищённости.



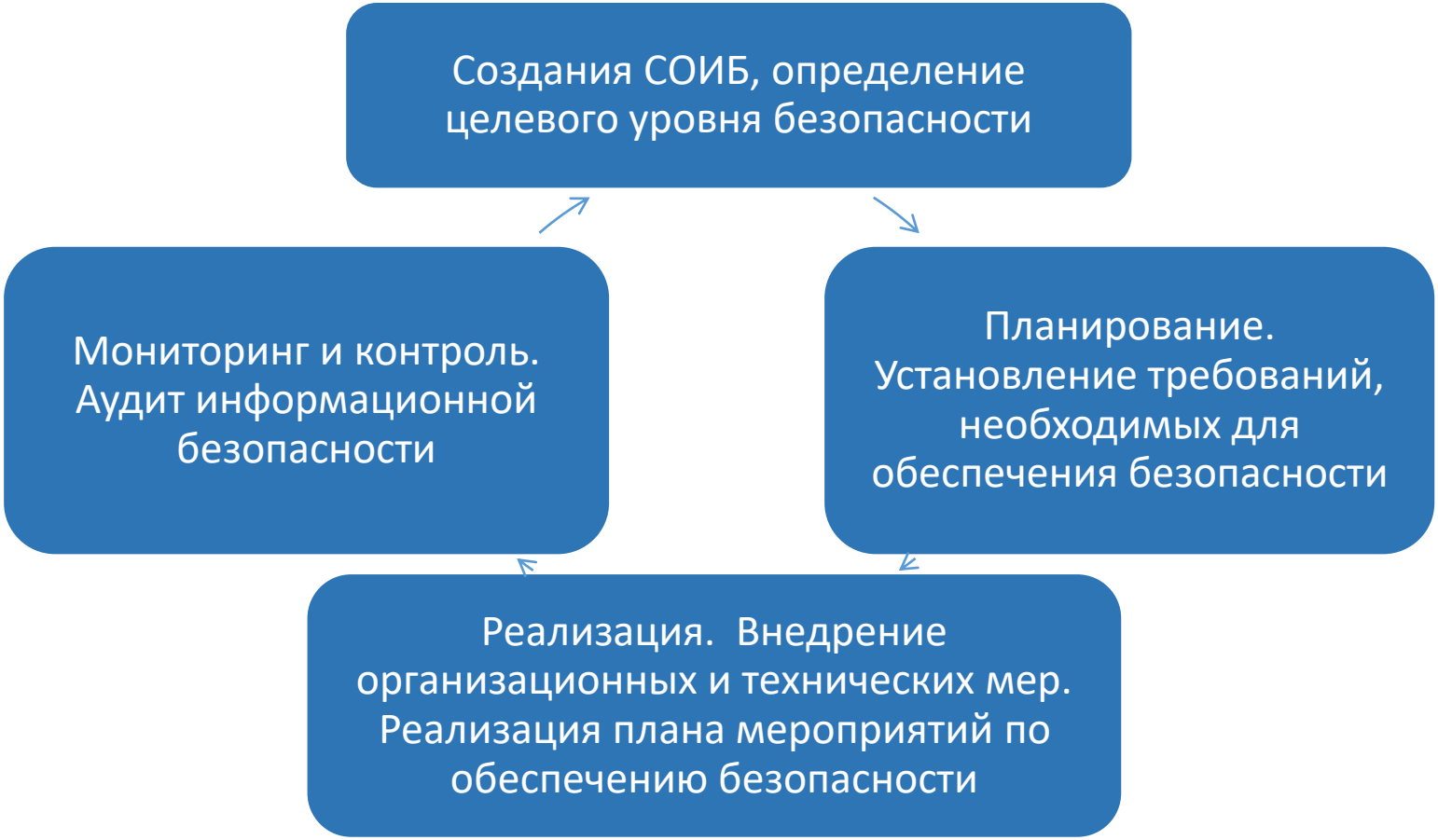
Категорирование объектов. Определение значимости

- Этап 1. Рассмотрение возможных действий нарушителей в отношении объектов КИИ и анализ угроз безопасности.
- Этап 2. Оценка объектов ИС в соответствии с показателями значимости и присвоение каждому из объектов ИС категории. Либо принятие решения об отсутствии необходимости её присвоения (первая, вторая и третья категории) экспертным путем.

Показатель	Значение показателя		
	III категория	II категория	I категория
Причинение ущерба жизни и здоровью людей (человек)	Более 1, но не менее или равно 50	Более 50, но не менее или равно 500	Более 500

Формирование требований к безопасности

- СЗИ должны соответствовать категории значимости. Необходимо следить за их адекватностью для противодействия как текущим угрозам, так и угрозам «нулевого дня».



Основные нормативно-правовые акты, устанавливающие меры защиты объекта

- Этап 1. Планирование.
- 1.1 Формирование плана организационно-распорядительных документов по безопасности, в том числе и методики по моделированию угроз и действий нарушителей.
- 1.2. Определение состава СЗИ их структуры, функций и требования к ним.
- 1.3 Формирование плана мероприятий, направленных на обеспечение безопасности.

Вид системы	Нормативно-правовые акты
АСУ	149-ФЗ, 31, 235, 239
ИТКС	149-ФЗ, 351, 235, 239, 17
МИС	149-ФЗ, 17, 235, 239
ГИС	149-ФЗ, 17, 235, 239
ИС Пнд	149-ФЗ, 152-ФЗ, 1119, 17, 235, 239, 378

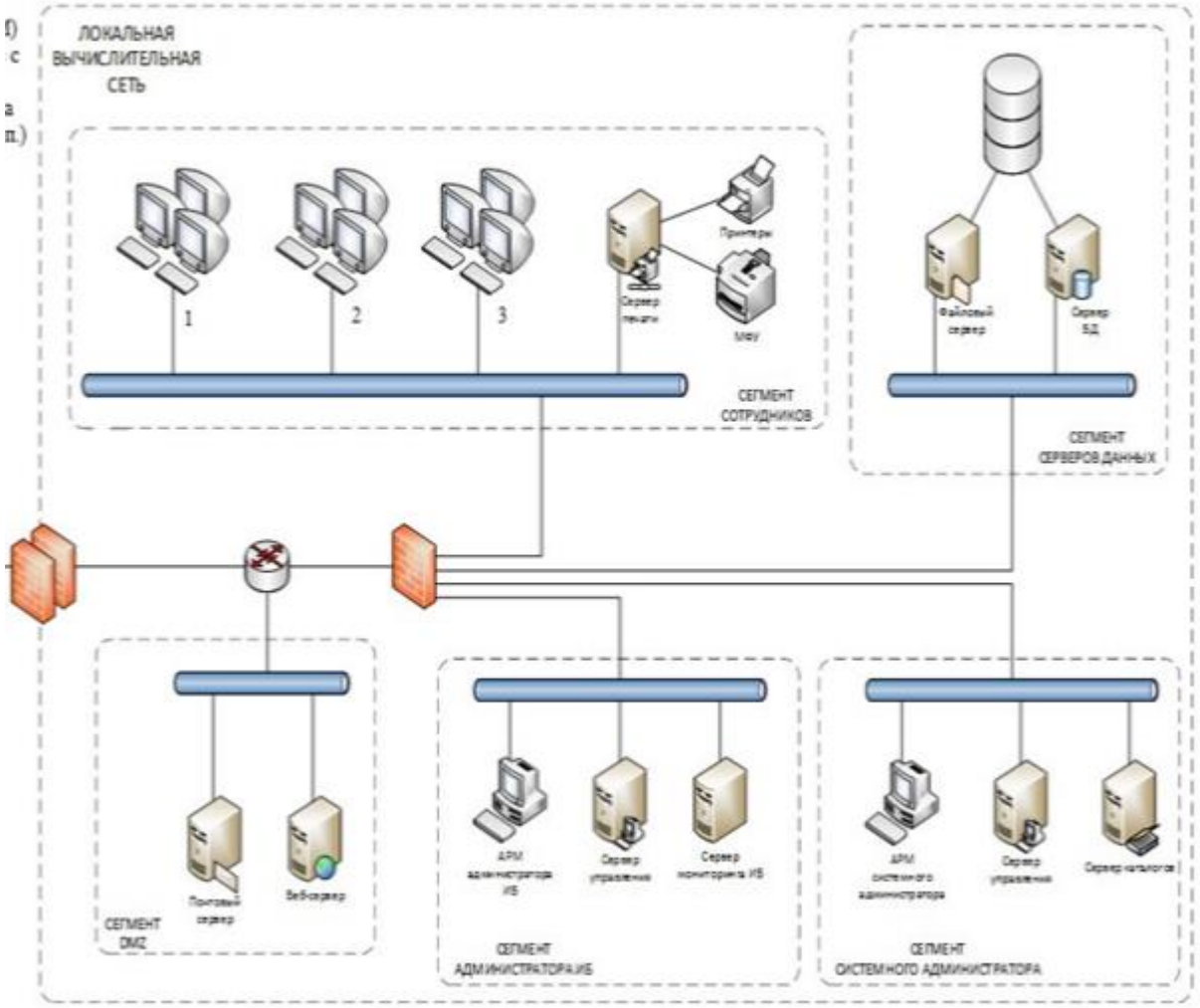
Реализация

Этап 2. Реализация. На данном этапе осуществляется внедрение организационных и технических мер, реализация плана мероприятий по обеспечению безопасности, в том числе:

- идентификация и аутентификация;
- управление доступом;
- аудит безопасности;
- антивирусная защита и управление обновлениями программного обеспечения;
- предотвращение вторжений (компьютерных атак) и реагирование на инциденты нарушений информационной безопасности;
- обеспечение целостности и доступности;
- защита технических средств и систем;
- защита информационной (автоматизированной) системы и ее компонентов;
- управление конфигурацией;
- планирование мероприятий по обеспечению безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Пример элементов многоуровневой системы обеспечения защиты при передаче информации по каналам связи

- Системы мониторинга сетей
- Системы обнаружения и предотвращения вторжений (IDS/IPS).
- Системы предотвращения утечек конфиденциальной информации (DLP системы).
- Анализаторы протоколов.
- Межсетевые экраны.
- Криптографические средства.
- Шифрование.
- Цифровая подпись.
- Системы резервного копирования.



Реализация

К мероприятиям по реализации целесообразно отнести:

1.Проверку готовности СЗИ к использованию, с составлением заключений о возможности эксплуатации СЗИ;

2.Введение в эксплуатацию СЗИ, в соответствии с эксплуатационной и технической документацией;

3.Обучение персонала работе с СЗИ;

4.Учет применяемых СЗИ, эксплуатационной и технической документации к ним;

5.Учет лиц, допущенных к работе с информацией;

6.Формирование нормативно-правовой документации при эксплуатации СЗИ.

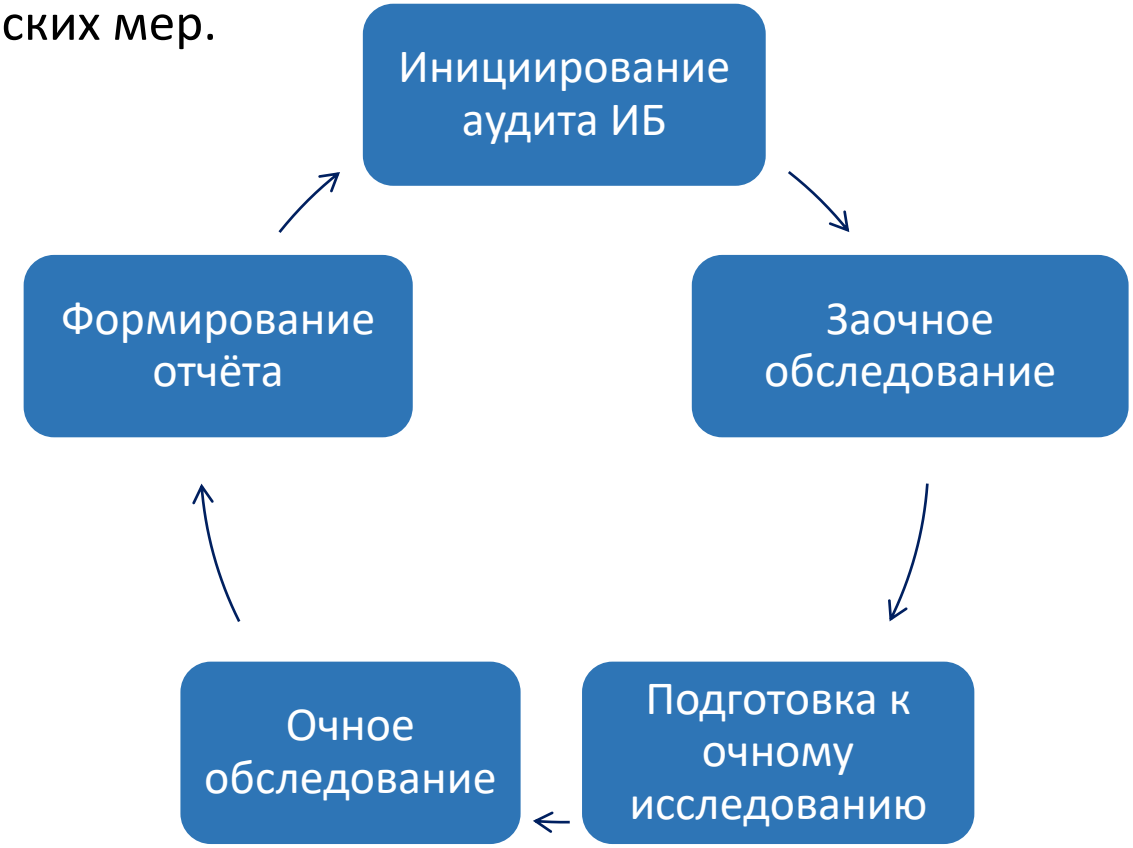
Мониторинг и контроль

К мероприятиям по мониторингу и контролю целесообразно отнести:

- проведение процедур, направленных на предотвращение несанкционированного доступа;
- своевременное обнаружение фактов НСД;
- предотвращение воздействий на технические средства обработки информации, в результате которых может быть нарушено их функционирование;
- незамедлительное восстановление информации, которая модифицирована или уничтожена в следствии несанкционированного доступа к ней;
- постоянный мониторинг за обеспечением уровня защищенности.

АУДИТ ИБ

В рамках контроля состояния безопасности должен осуществляться аудит ИБ, с оценкой эффективности принимаемых организационных и технических мер.



Литература. Основные нормативно-правовые акты

- 149-ФЗ - Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- 152-ФЗ - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- 1119 - Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- 351 - Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно телекоммуникационных сетей международного информационного обмена».
- 17 - Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
- 21 - Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Литература. Основные нормативно-правовые акты

- 31 - Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 09.08.2018) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
- 235 - Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования»
- 239 - Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ»
- 378 - Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности.