Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

Защита информации

Политика информационной безопасности в организациях

КУТУЗОВ Виктор Владимирович

Республика Беларусь, Могилев, 2024

Безопасность

- **Безопасность** есть отсутствие опасности, сохранность, надежность [Толковый словарь В. Даля]
- **Безопасность** – это состояние при котором не угрожает опасность, есть защита от опасности [Толковый словарь С. Ожегова]
- **Безопасность** – возможность продолжения существования системы (отсутствие возможности ее гибели или причинения ей неприемлемого ущерба). [Информационный бюллетень Межпарламентской Ассамблеи СНГ, 2014 г., № 61]
- **Безопасность** – отсутствие недопустимого риска, связанного с возможностью причинения вреда и (или) нанесения ущерба [Национальный правовой Интернет-портал Республики Беларусь, 24.10.2014, 3/3050]

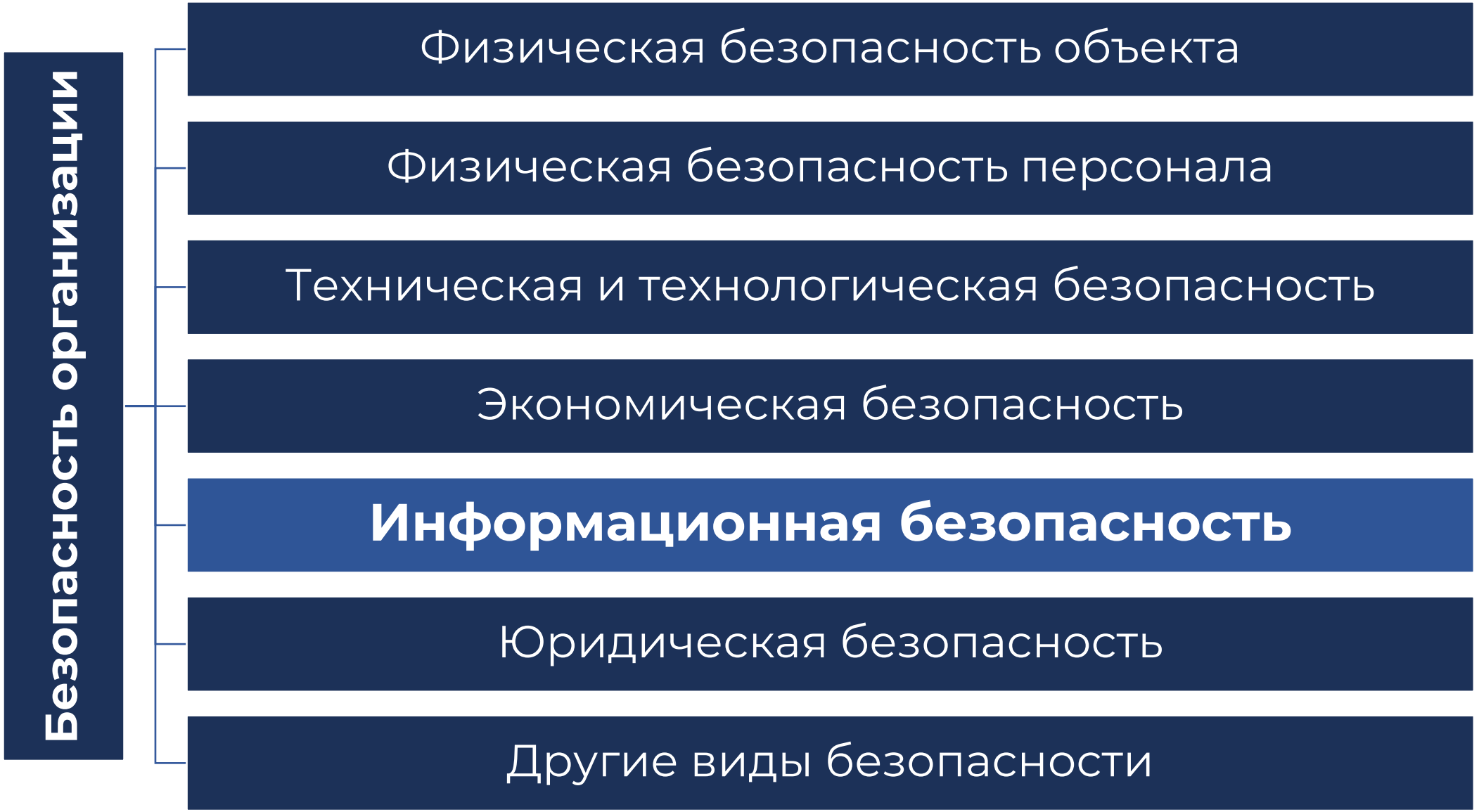
Безопасность

- **Безопасность** – результат деятельности по обеспечению безопасности.
  - **В одном случае** – это способность системы предотвращать ущерб жизненно важным интересам личности, общества, организации государства и международного сообщества в целом.
  - **В другом случае** – состояние защищенности системы.
  - **В третьем** – свойство развитой системы мер безопасности.

Безопасность предприятия

- **Безопасность предприятия** это состояние защищенности материальных ценностей и информационных ресурсов, штатного персонала и посетителей предприятия от внутренних и внешних угроз, а совокупность мер, направленных на реализацию такого состояния, называют системой безопасности предприятия.
- Она включает в себя:
  - юридическую защиту законных интересов предприятия от противоправных посягательств;
  - охрану жизни и здоровья персонала от воздействия последствий техногенных аварий;
  - экономическую защиту - сохранение финансовых и материальных средств, других ценностей от хищения, повреждения и уничтожения;
  - защиту конфиденциальной информации от утечки, искажения, уничтожения (информационная безопасность);
  - защиту от угроз со стороны технических средств обеспечения производственного (технологического) процесса и жизнедеятельности предприятия (энергоснабжение, вентиляция, водоснабжение, сосуды с высоким давлением, высокотемпературные технологические процессы и т.п.);
  - страхование рисков;
  - и многое др.

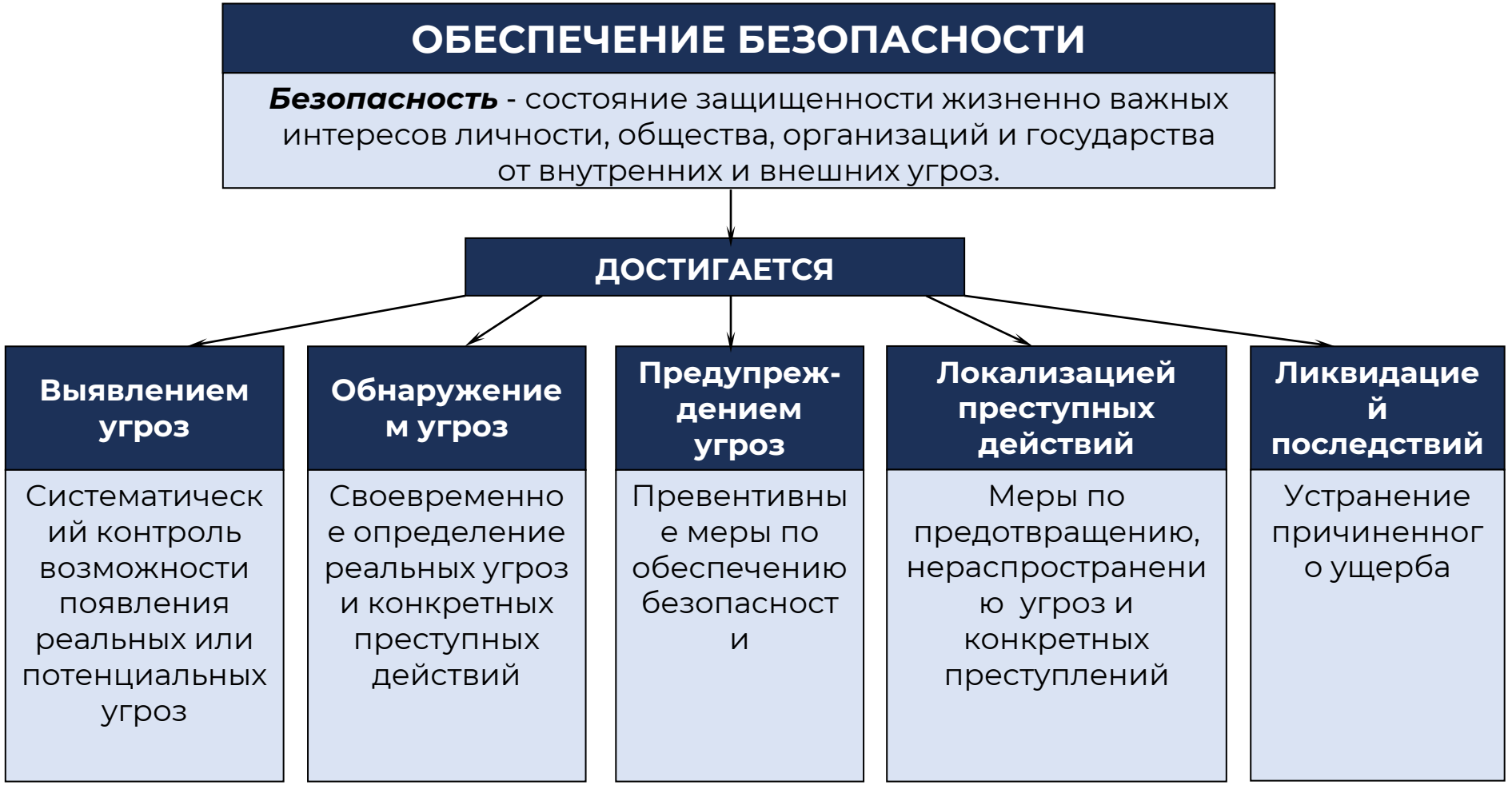
Обеспечение безопасности организации и её персонала



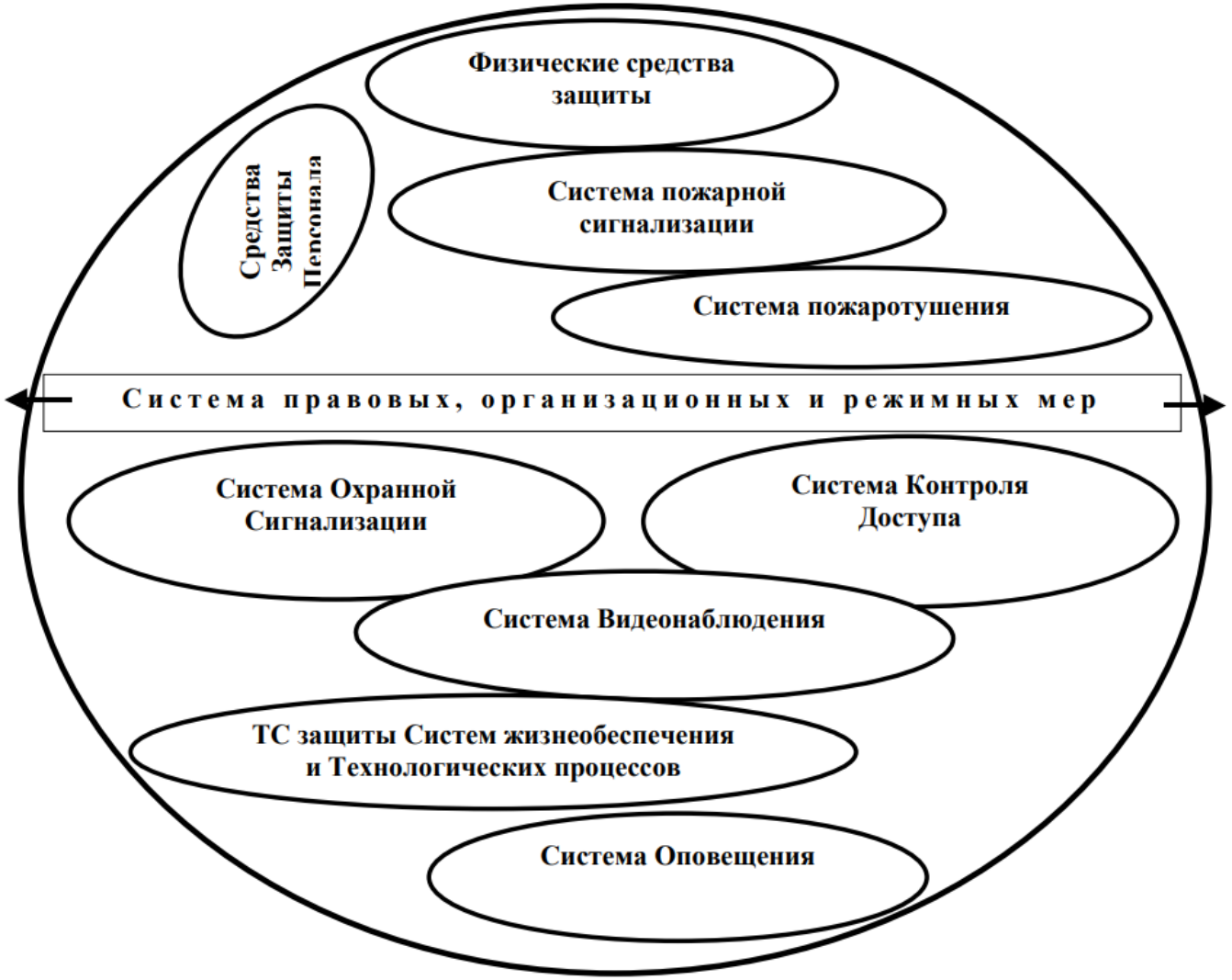
Обеспечение безопасности

- **Обеспечение безопасности** – деятельность индивидов, организаций, обществ, государства, мирового сообщества в целом по выявлению, предупреждению и отражению угроз (опасностей), способных нанести ущерб, лишить материальных и духовных ценностей, закрыть путь для выживания и прогрессивного развития, погубить их.
- В этом случае опасность становится объектом деятельности по обеспечению безопасности.

Схема деятельности по обеспечению безопасности



Основные составляющие систем безопасности предприятия (организации)



Основные составляющие систем безопасности предприятия (организации)

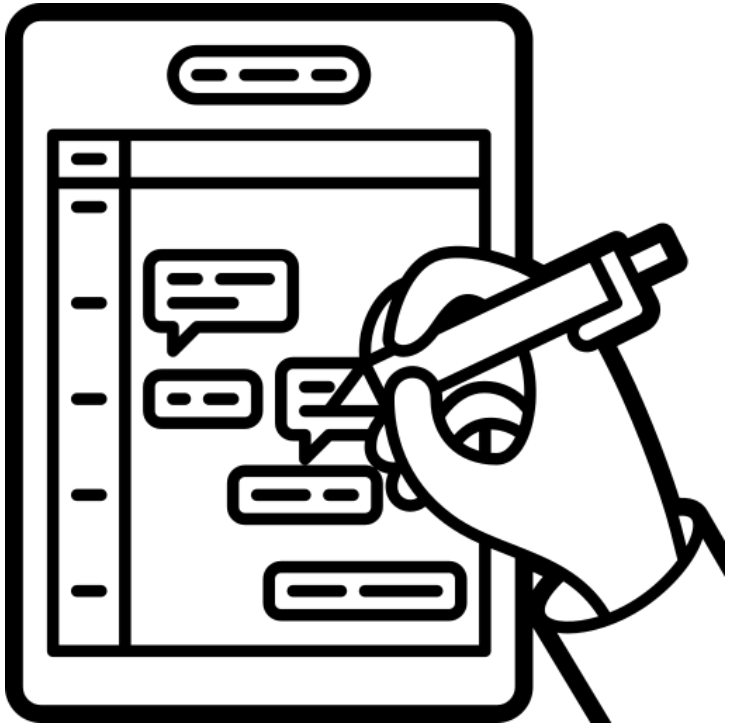
- **К системе безопасности предприятия можно отнести комплекс правовых, организационных и режимных мер и системы технических средств защиты**, которые на данном предприятии разработаны, внедрены и поддерживаются.
- **Основными из них принято считать:**
- **комплекс внутренних документов предприятия**, определяющих поведение каждого члена коллектива в отдельности и взаимодействие отдельных исполнителей и подразделений в течение всего срока жизнедеятельности предприятия в различных ситуациях (правовых, организационных, режимных);

Основные составляющие систем безопасности предприятия (организации)

- **комплекс технических и технологических документов**, определяющих порядок и условия выполнения как отдельных технологических операций, так и всех технологических процессов производства на данном предприятии;
- **комплекс систем и технических средств защиты**, который в свою очередь состоит из:
  - систем и средств физической защиты объекта,
  - систем охранно-пожарной сигнализации,
  - систем управления доступом,
  - систем охранного видеонаблюдения,
  - технических средства защиты инженерных систем жизнеобеспечения здания и опасных технологических процессов,
  - систем пожаротушения и дымоудаления,
  - технических средства защиты персонала, в том числе средства индивидуальной защиты,
  - систем защиты информации.
  - систем оповещения.

Обеспечение безопасности

- Для работы по обеспечению безопасности используются разные формы организации подразделений и специалистов. **Чаще применяется вариант самостоятельного решения своих задач отдельными подразделениями**.
- **Например**: **юридическая служба (или юрист)** решает свои задачи, анализируя все основные договоры предприятия с внешними партнерами и коллективом предприятия;
- **технологическая служба** обеспечивает контроль за опасными технологическими процессами;
- **служба энергетика** контролирует состояние и развитие систем энергоснабжения, вентиляции, лифтов и т.д.
- На предприятиях существует также **служба безопасности**, которая контролирует состояние и развитие **в основном технических средств охраны, пожарной автоматики и защиты информации**.
- Иногда функции контроля пожарной и охранной сигнализации поручают **службе ведомственной связи** (АТС).

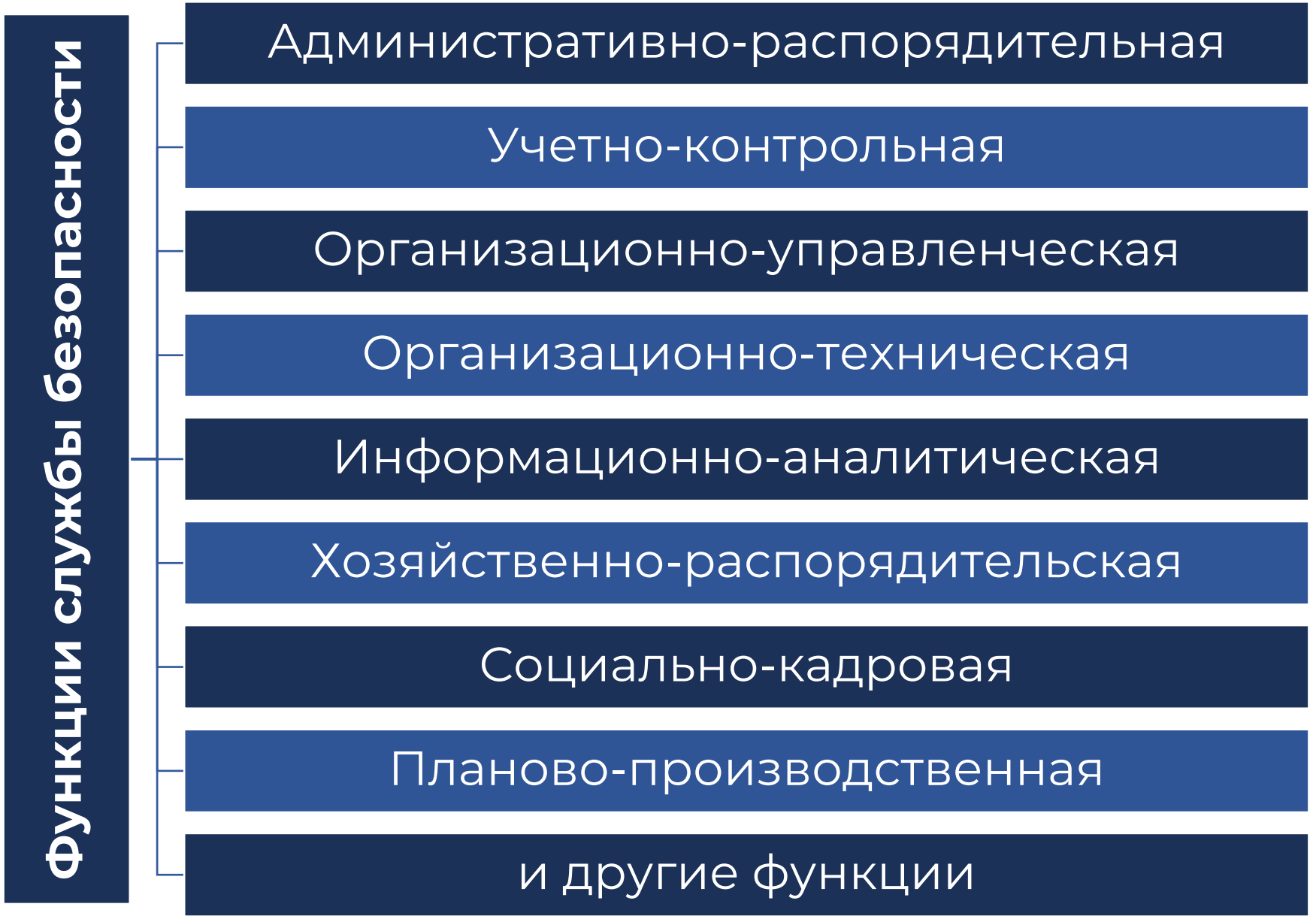


1. Служба безопасности предприятия (организации)

Служба безопасности

- **Служба безопасности (СБ)** является структурным подразделением, организуемым администрацией для обеспечения целостности технико-технологических, экономических, правовых, коммерческих, режимных и физических компонентов предприятия, организации, учреждения.
- Она формируется на основе анализа, оценки и прогнозов их внутренней деятельности с целью решения задач защиты интересов предприятия.
- Ее статус определяется соответствующим приказом руководителя предприятия либо решением вышестоящей организации, в которую входит это предприятие.

Функции службы безопасности



Примерное содержание функций службы безопасности

- **административно-распорядительная функция** - реализуется путем подготовки решений по установлению и поддержанию системы безопасности, определению полномочий, прав, обязанностей и ответственности должностных лиц по вопросам обеспечения безопасности объекта;

- **хозяйственно-распорядительная функция** - реализуется путем участия службы безопасности в определении ресурсов, необходимых для решения задач безопасности объекта, в подготовке и проведении мероприятий по обеспечению сохранности имущества, финансовой, интеллектуальной и иной собственности;

Примерное содержание функций службы безопасности

- **учетно-контрольная функция** - реализуется выделением наиболее важных направлений финансово-коммерческой деятельности предприятия и работой по организации своевременного обнаружения внешних и внутренних угроз финансовой стабильности и устойчивости объекта, оценкой их источников, налаживанием контроля за критическими ситуациями, ведением учета негативных факторов, влияющих на безопасность объекта, а также накоплением информации о недобросовестных конкурентах, ненадежных партнерах, лицах и организациях, посягающих на жизненно важные интересы объекта;

Примерное содержание функций службы безопасности

- **социально-кадровая функция** - реализуется участием службы безопасности в подборе и расстановке кадров, выявлении негативных тенденций, возможных причин и условий социальной напряженности, в предупреждении и локализации конфликтов, создании нормальной обстановки, инструктаже персонала объекта по вопросам своей компетенции, формировании у него чувства ответственности за соблюдение установленных режимов безопасности;

Примерное содержание функций службы безопасности

- **организационно-управленческая функция** – реализуется путем создания и эффективного поддержания организационной структуры управления процессом обеспечения безопасности, гибких временных структур по отдельным направлениям работы, организации взаимодействия и координации между отдельными звеньями системы для достижения заданных программных целей;

Примерное содержание функций службы безопасности

- **планово-производственная функция** - реализуется путем разработки комплексной программы и отдельных подсистемных целевых планов обеспечения безопасности объекта, подготовки и проведения мероприятий по их осуществлению, установлению и поддержанию режимов безопасности;
- **организационно-техническая функция** - реализуется путем организации материально-технического и финансового обеспечения системы безопасности объекта, применением специальной техники и достижений соответствующих текущим потребностям предприятия, содействием в освоении сотрудниками предприятия новых видов техники для специальной деятельности;

Примерное содержание функций службы безопасности

- **информационно-аналитическая функция** – реализуется целенаправленным сбором, накоплением и обработкой информации, относящейся к сфере безопасности, созданием и использованием необходимых для этого технических и методических средств аналитической обработки информации, организацией информационного обеспечения заинтересованных подразделений и отдельных лиц в сведениях, имеющихся в службе безопасности.

Обеспечение экономической безопасности компании

Взаимодействие

Служба безопасности компании

Отдел экономической безопасности

5

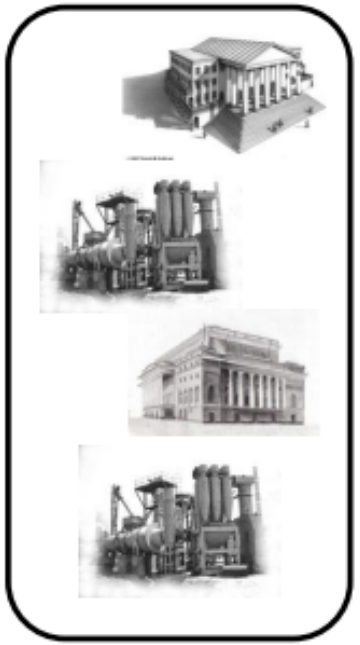
Реализация политики экономической безопасности

Уполномоченные государственные органы

1) Изучение контрагентов
2) Мониторинг контрагентов
3) Возврат просроченной задолженности
4) Изучение рынка и конкурентов
5) Защита коммерческой тайны
6) Предотвращение внешнего мошенничества и иных корыстных правонарушений
7) Выявление возможных действий, направленных на нанесение экономического ущерба
8) Выявление попыток подготовки и проведения рейдерских захватов
9) Взаимодействие с заинтересованными подразделениями компании
10) Взаимодействие с правоохранительными органами в целесообразных случаях
11) Содействие формирования мер, направленных на предупреждение негативных проявлений и минимизацию их последствий

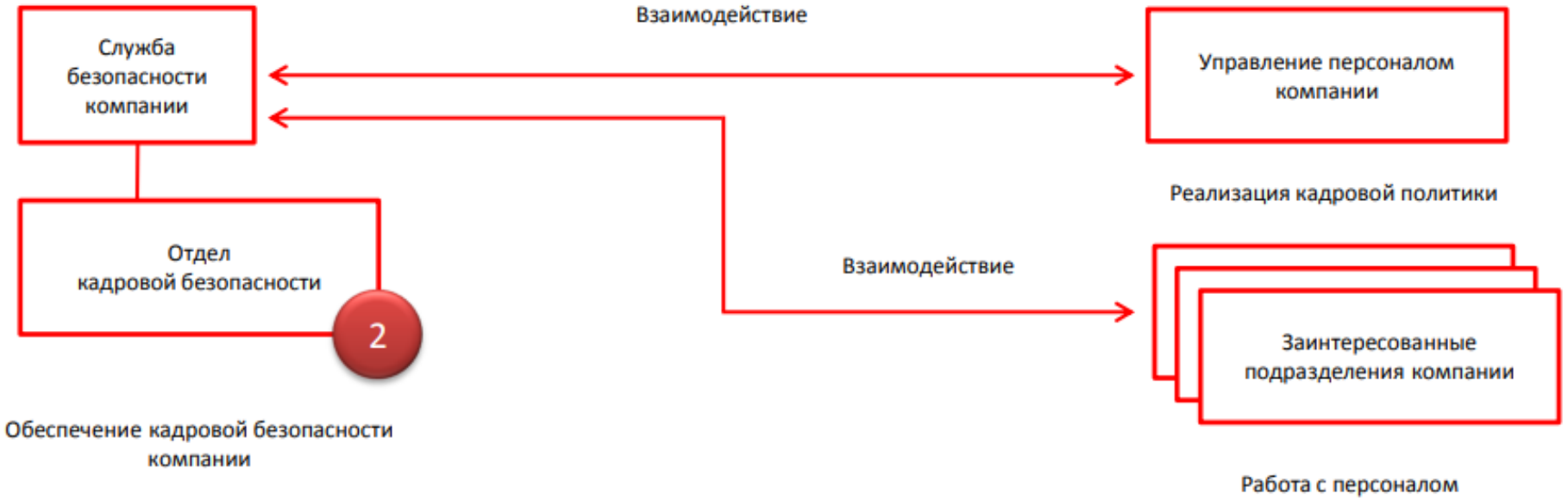
Заинтересованные подразделения компании

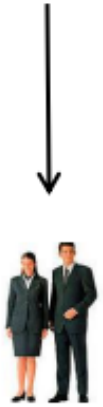
Реализация производственных функций



Контрагенты и конкуренты

Обеспечение кадровой безопасности компании





Уполномоченные государственные органы

Противодействие коррупции

Изучение персонала на различных стадиях кадрового процесса:

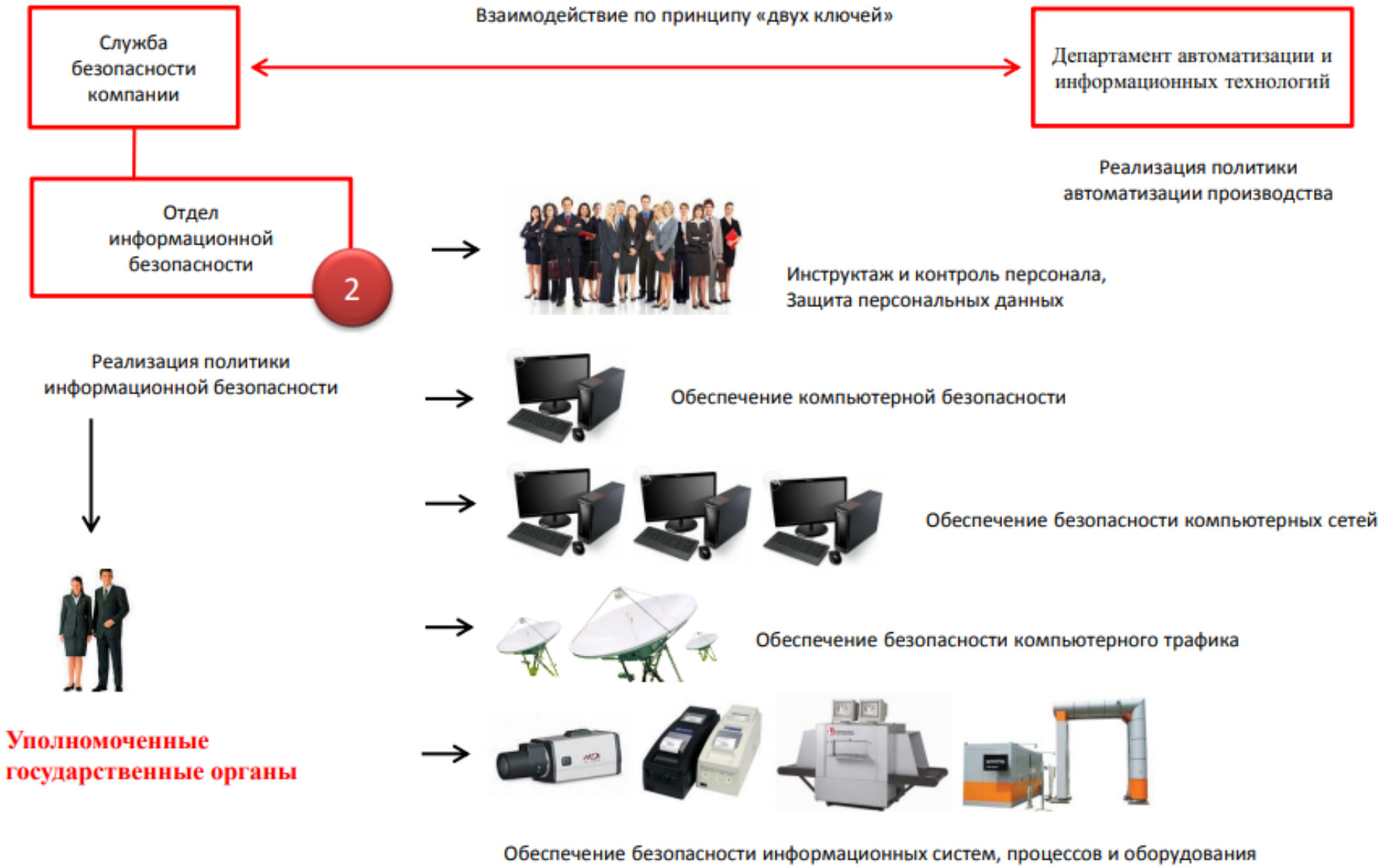
А) при приеме

Б) в процессе работы

В) проведение внутренних служебных расследований

Г) при увольнении

Обеспечение информационной безопасности компании



Матрица SWOT-анализа для системы безопасности промышленного предприятия

Экономическая безопасность

+ средняя квалификация сотрудников
+ договор с бюро кредитных историй
+ наличие собственной базы данных

- поверхностная проверка контрагентов
- недоработки клиентских служб
- отсутствие общего нормативного документа о порядке изучения потенциальных партнеров

Финансовая безопасность

+ высокая квалификация сотрудников
+ эффективный бухгалтерский контроль

- нет функции внутреннего аудита
- замечания от банка по нецелевому использованию кредита
- выявлена попытка размещения на счете транзитных средств, подозрительная на отмывание

Информационная безопасность

+ закуплено современное оборудование
+ установлены программные средства

- нет подготовленных специалистов
- функции автоматизации и ИБ не разделены
- похищены средства с электронного счета компании
- сотрудники используют ПК для игр в Интернете

Физическая безопасность

+ штаты охраны укомплектованы
+ сотрудники имеют лицензии
+ получено служебное оружие
+ сотрудники уверенно владеют штатными досмотровыми средствами

- получены замечания по оборудованию оружейной комнаты
- низкая профессиональная подготовка личной охраны генерального директора

Инженерно-техническая безопасность

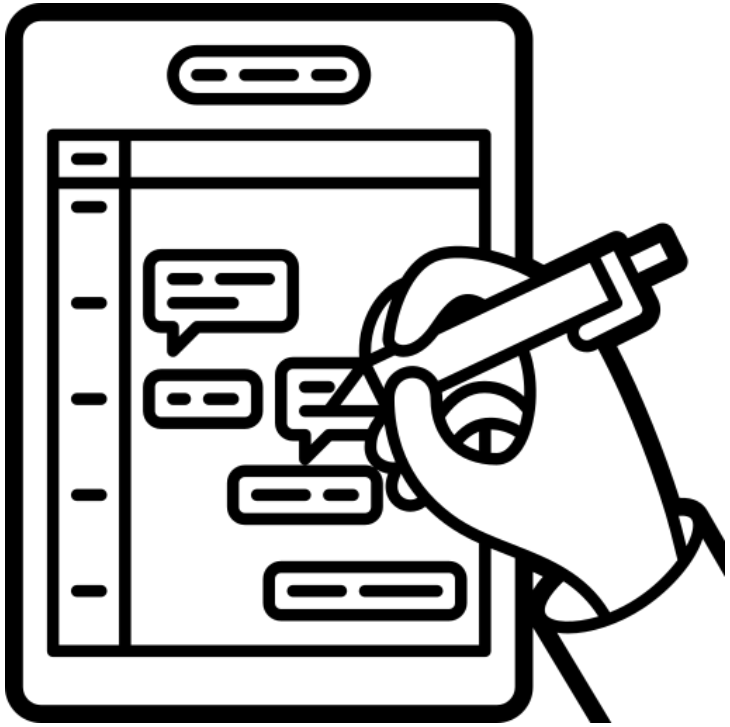
+ входы для работников оснащены СКУД
+ въезды оснащены средствами досмотра
+ периметр оснащен средствами контроля
+ склады оснащены средствами контроля

- устарели средства видео-контроля
- подлежат замене огнетушители
- предписано автоматизировать средства пожаротушения в литейном цехе

Кадровая безопасность

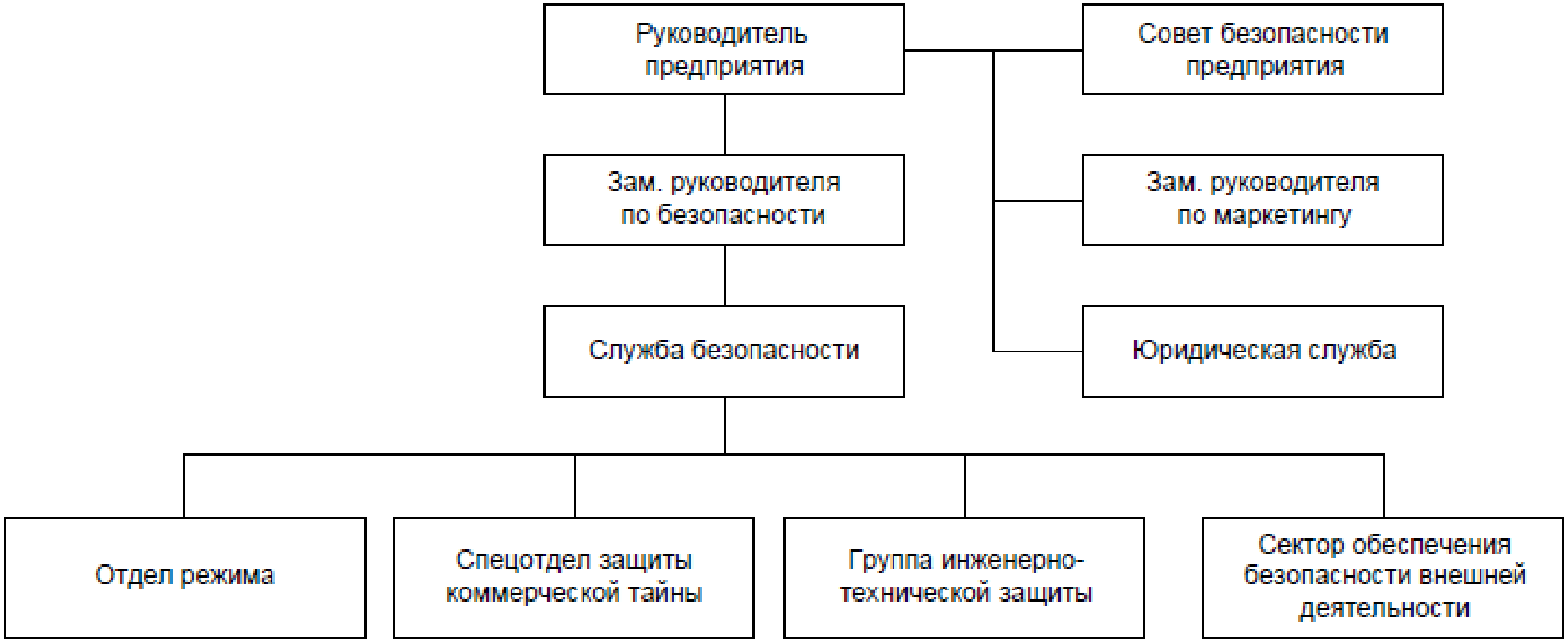
+ утверждено положение о порядке подбора и изучения персонала
+ утверждено положение о порядке использования полиграфа
+ введена штатная должность оператора полиграфа
+ закуплен и введен в эксплуатацию полиграф

- не выявлены организаторы схемы отмывания денежных средств



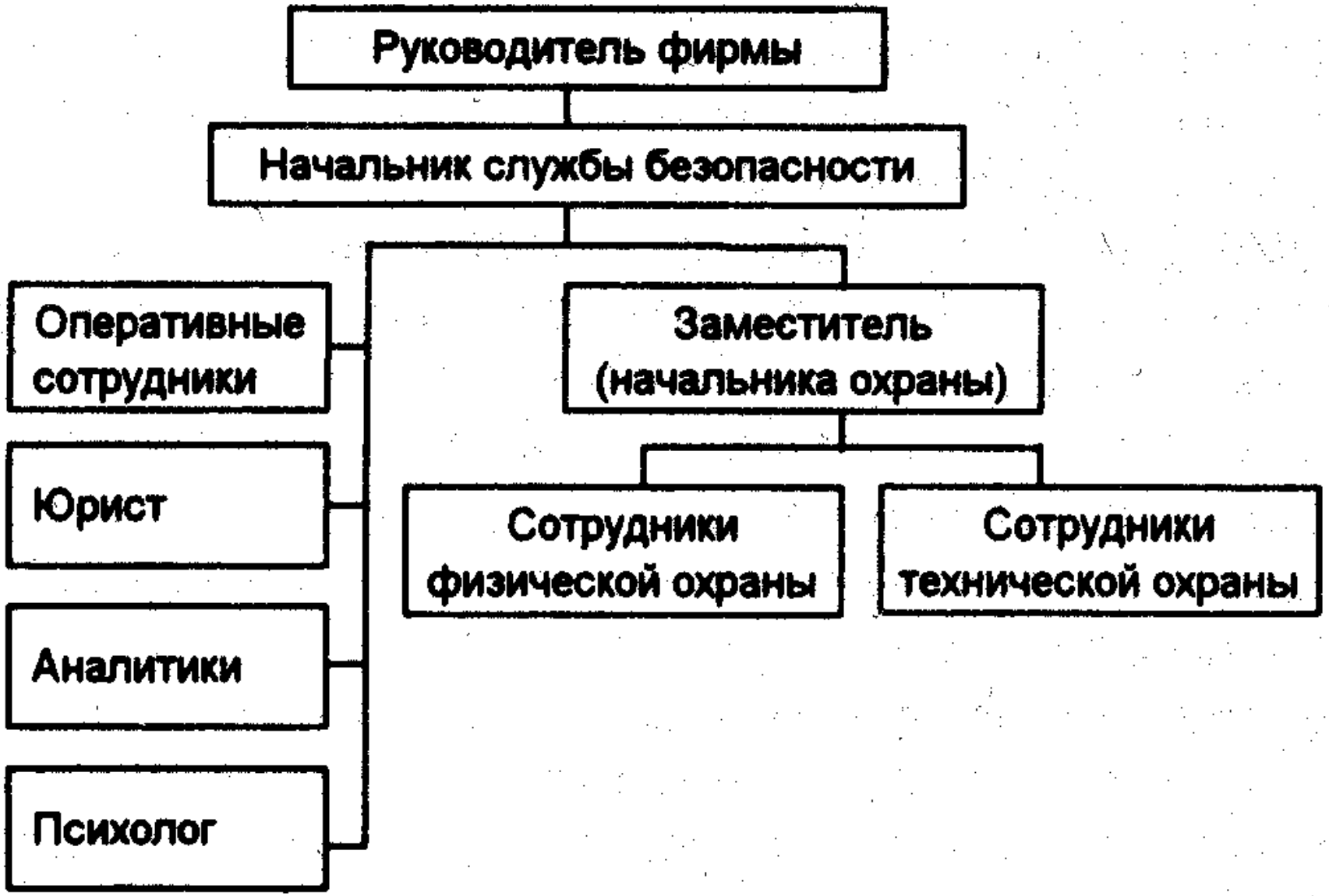
2. Пример структуры службы безопасности

Пример структуры службы безопасности

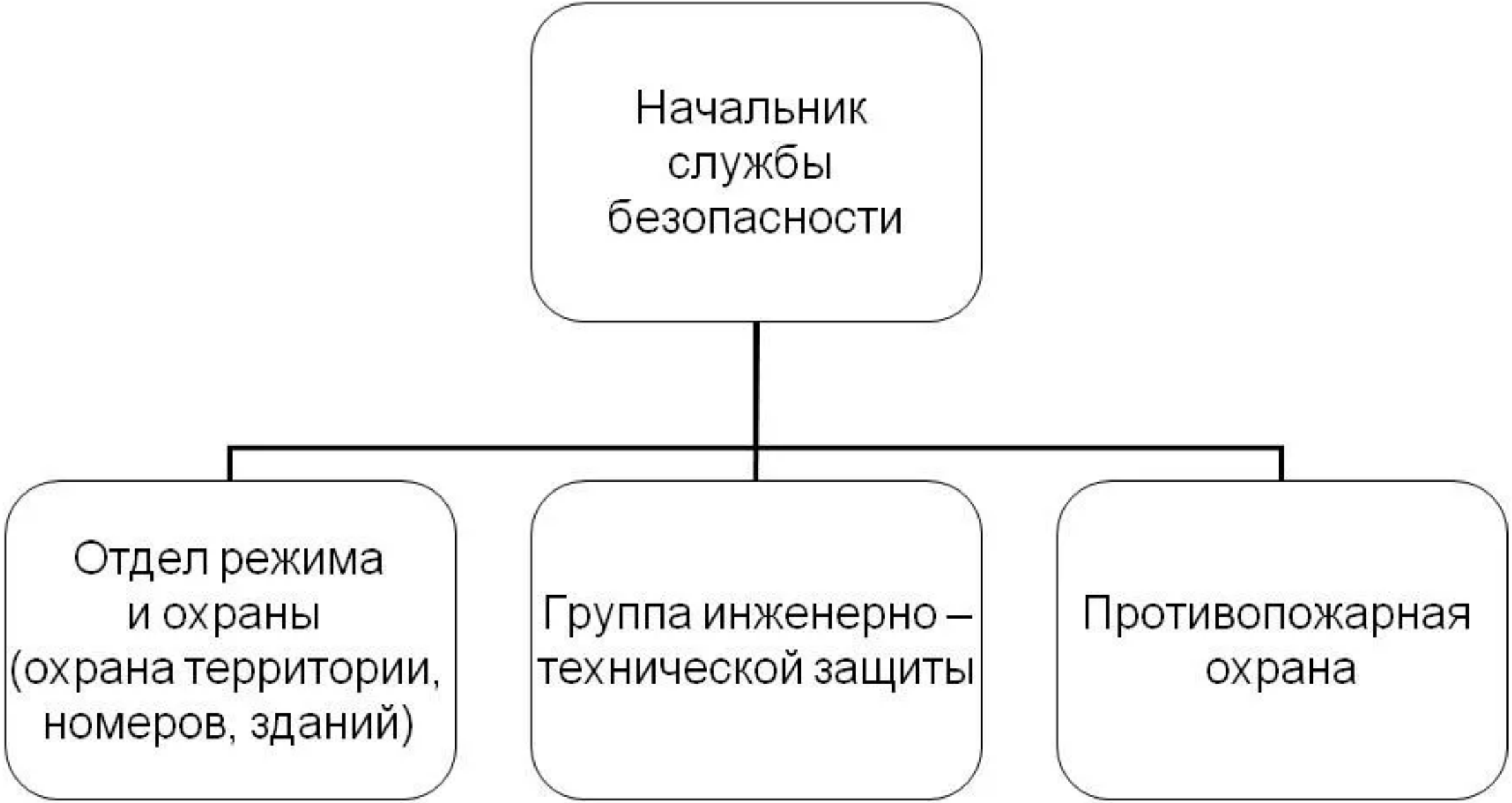


Пример структуры службы безопасности

Пример структуры службы безопасности

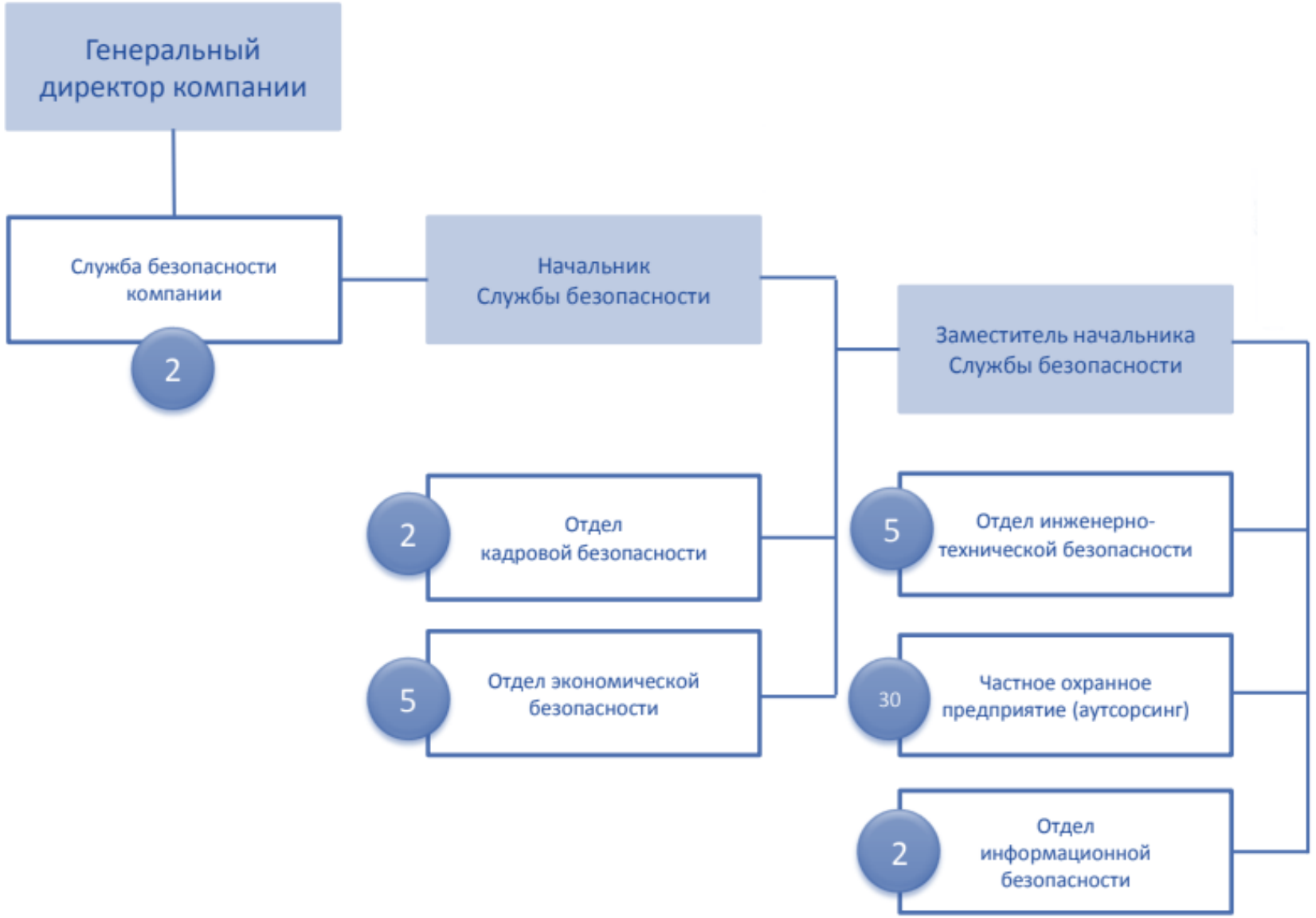


Пример структуры службы безопасности



Пример структуры службы безопасности

Пример структуры службы безопасности



Этапы создания системы безопасности предприятия (организации)

- **При создании системы безопасности предприятия** (организации) необходимо придерживаться следующей **последовательности**:

  1. Определение ценностей, представляющих интерес для противника, оценка потенциальных противников (потенциально возможных угроз и степени их важности).

  2. Оценка степени угрозы тем или иным ценностям (секретам), выявление каналов утечки информации, вариантов потери материальных и нематериальных активов предприятия, вариантов возможных угроз сотрудникам, окружающей среде, третьим лицам.

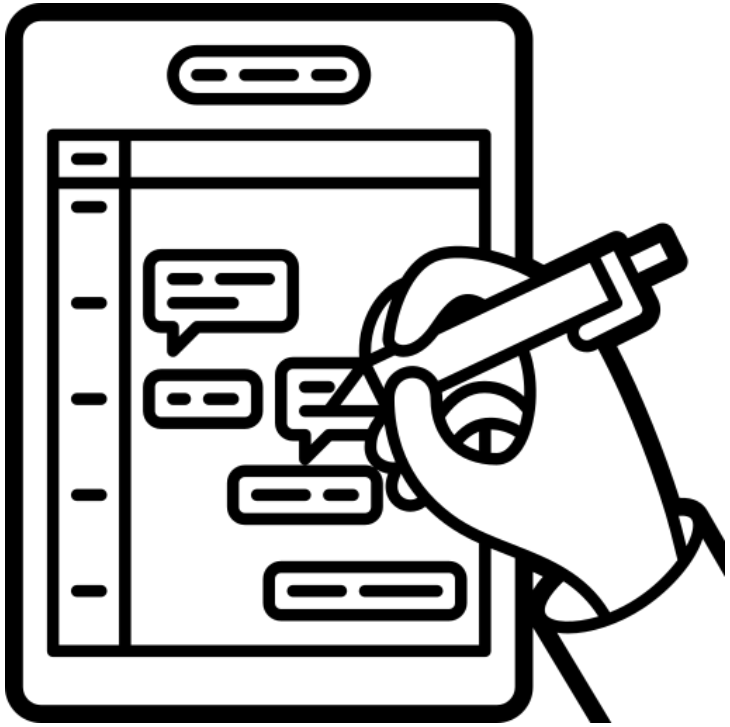
  3. Оценка уязвимых мест (точек) методом системного анализа.

  4. Сопоставление уязвимых мест с конкретными угрозами для оценки степени риска, оценка ожидаемых убытков.

  5. Выработка контрмер для защиты. Разработка организационно-штатной структуры системы безопасности, приобретение и установка программных и технических средств защиты, составление программы страховой защиты предприятия, определение экономической эффективности принимаемых мер.

  6. Организованная эксплуатация системы. Создание максимально удобных условий для пользователей системы безопасности, обеспечение установленного порядка эксплуатации технических средств безопасности, контроль за соблюдением организационных требований системы.

- С появлением новых ценностей, требующих защиты или с появлением новых угроз для имеющихся ценностей эта последовательность действий повторяется.



3. Электронные средства охраны, безопасности и контроля

Электронные средства охраны, безопасности и контроля

- Техническую основу обеспечения охраны и безопасности составляют электронные средства охраны.

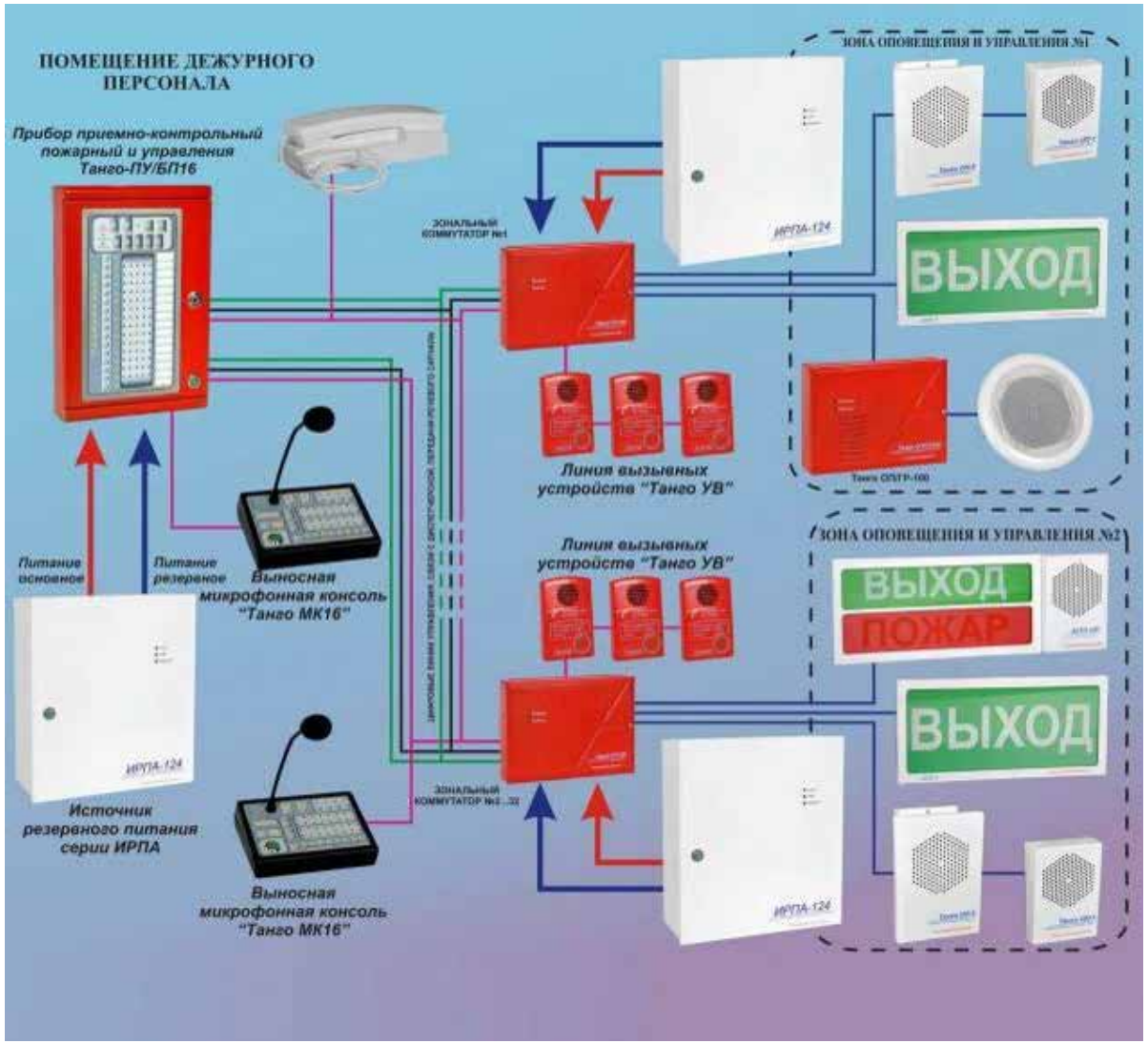
- К ним относятся:
  - системы охранной и пожарной сигнализации;
  - системы контроля доступа;
  - системы видеонаблюдения.

- Они могут работать как по отдельности, так и в комплексе.

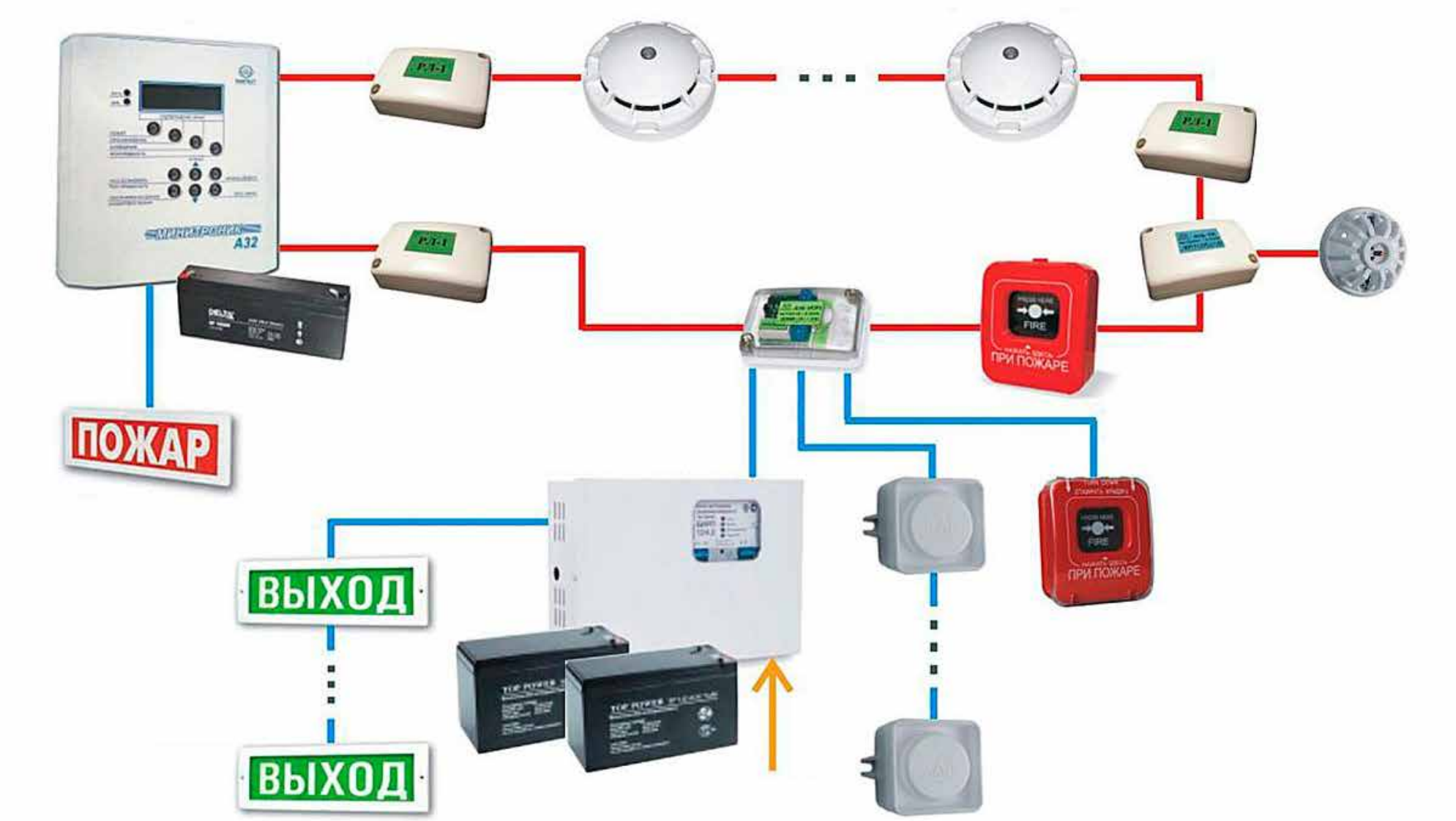
Состав электронных средств охраны

Состав электронных средств охраны

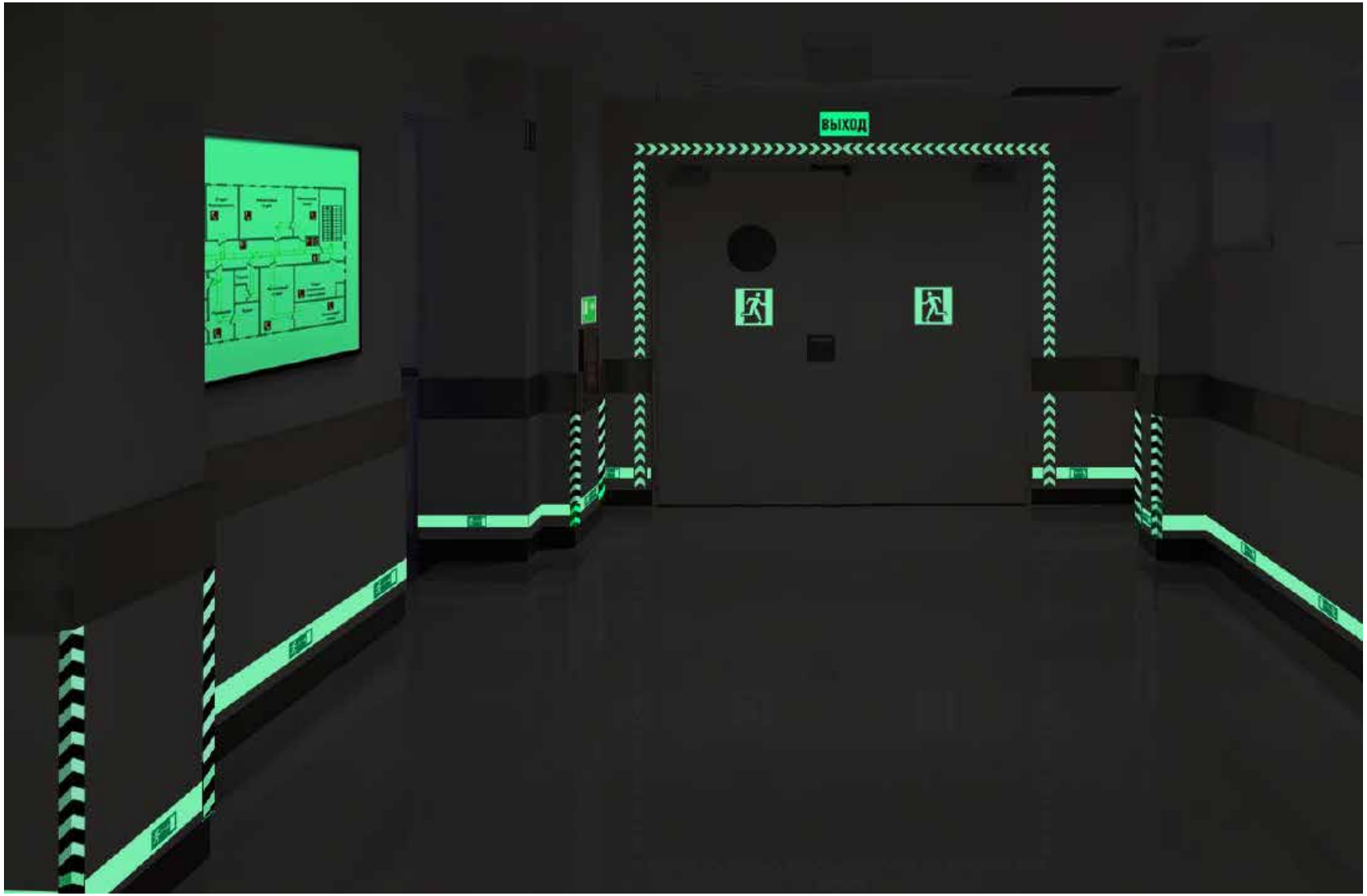
Система оповещения людей о пожаре и управления эвакуацией



Система оповещения людей о пожаре и управления эвакуацией



Система оповещения людей о пожаре и управления эвакуацией



Состав электронных средств охраны

Системы контроля доступа

Системы контроля доступа

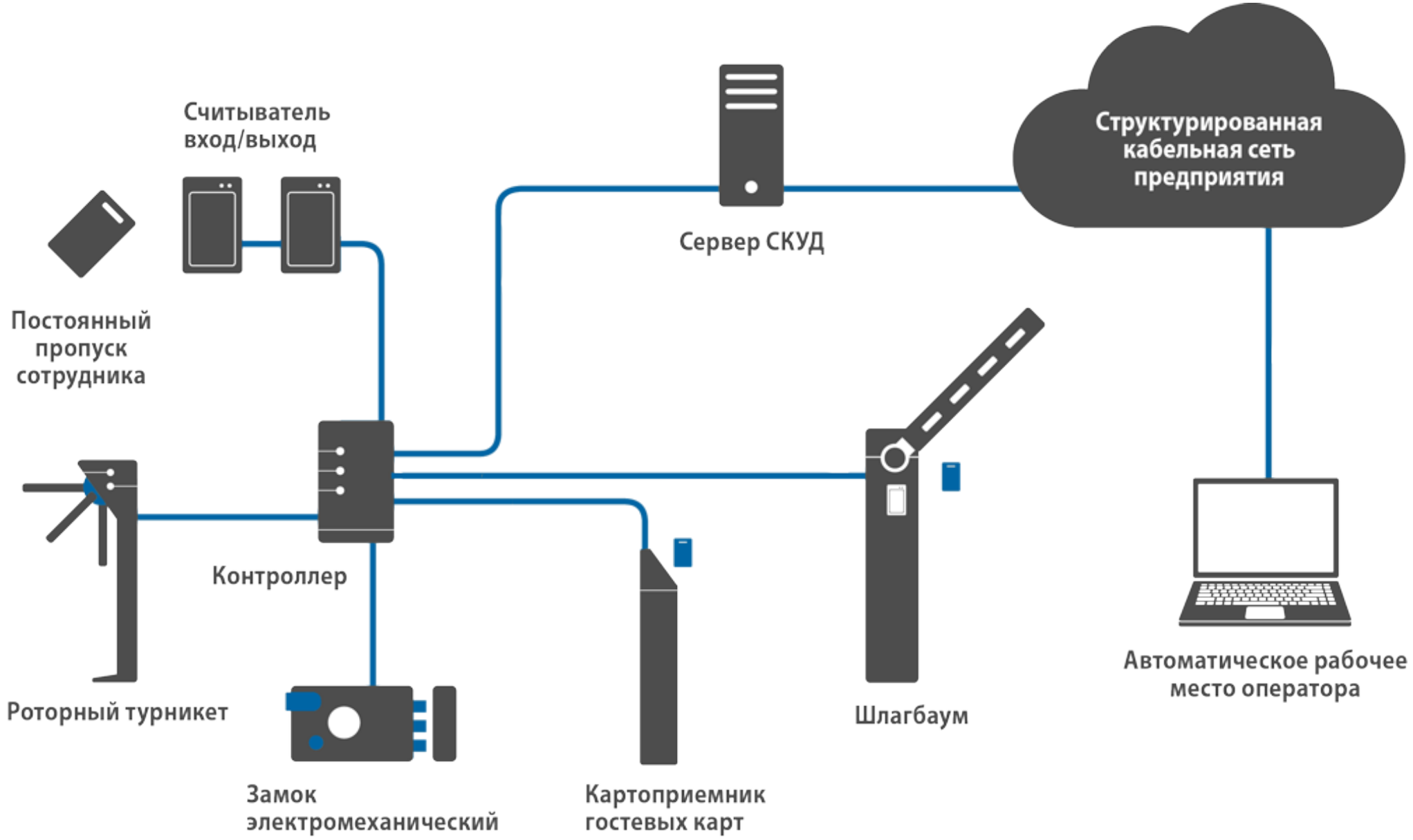
Системы контроля доступа

Системы контроля доступа

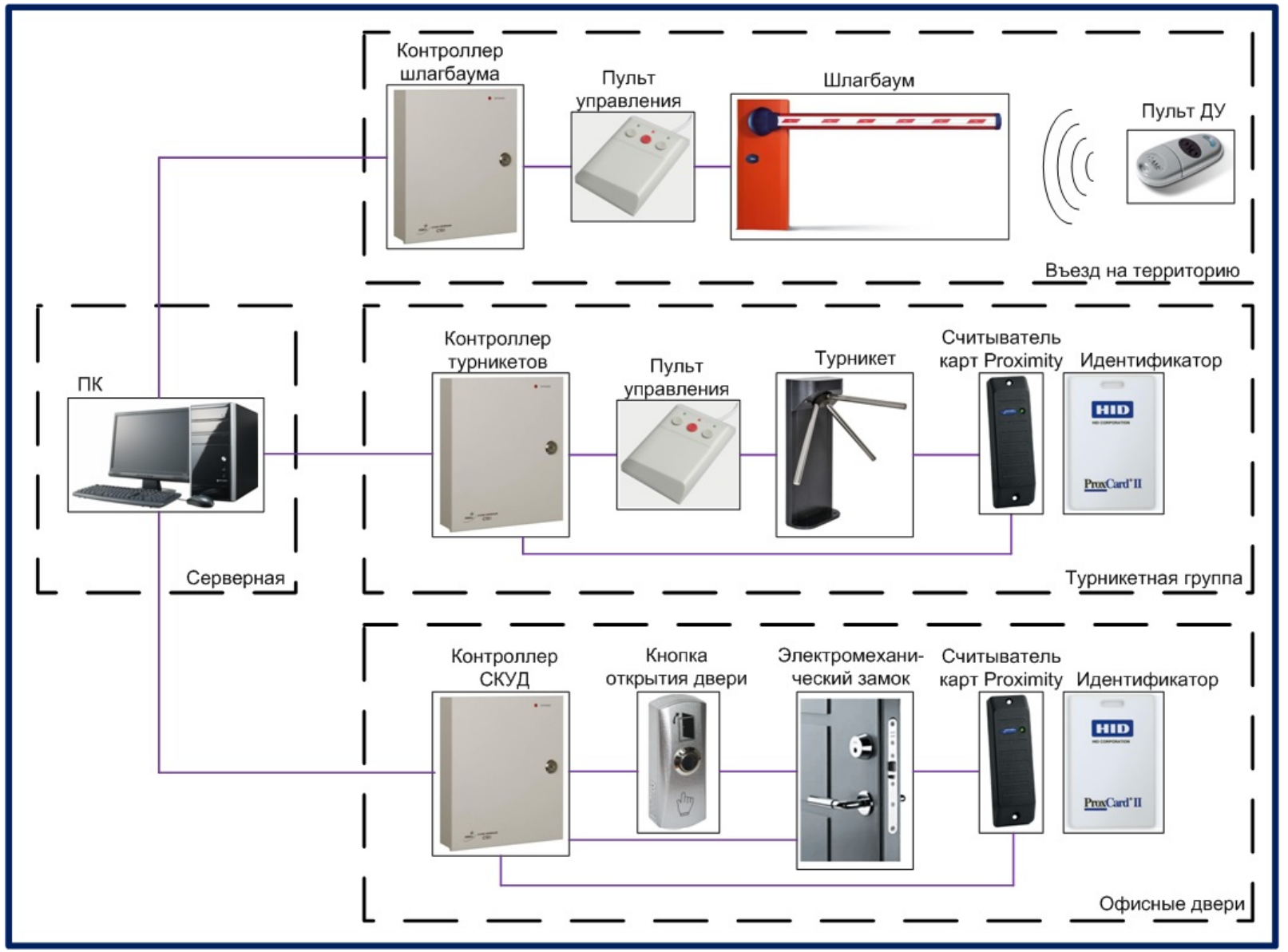
Системы контроля доступа

Системы контроля доступа

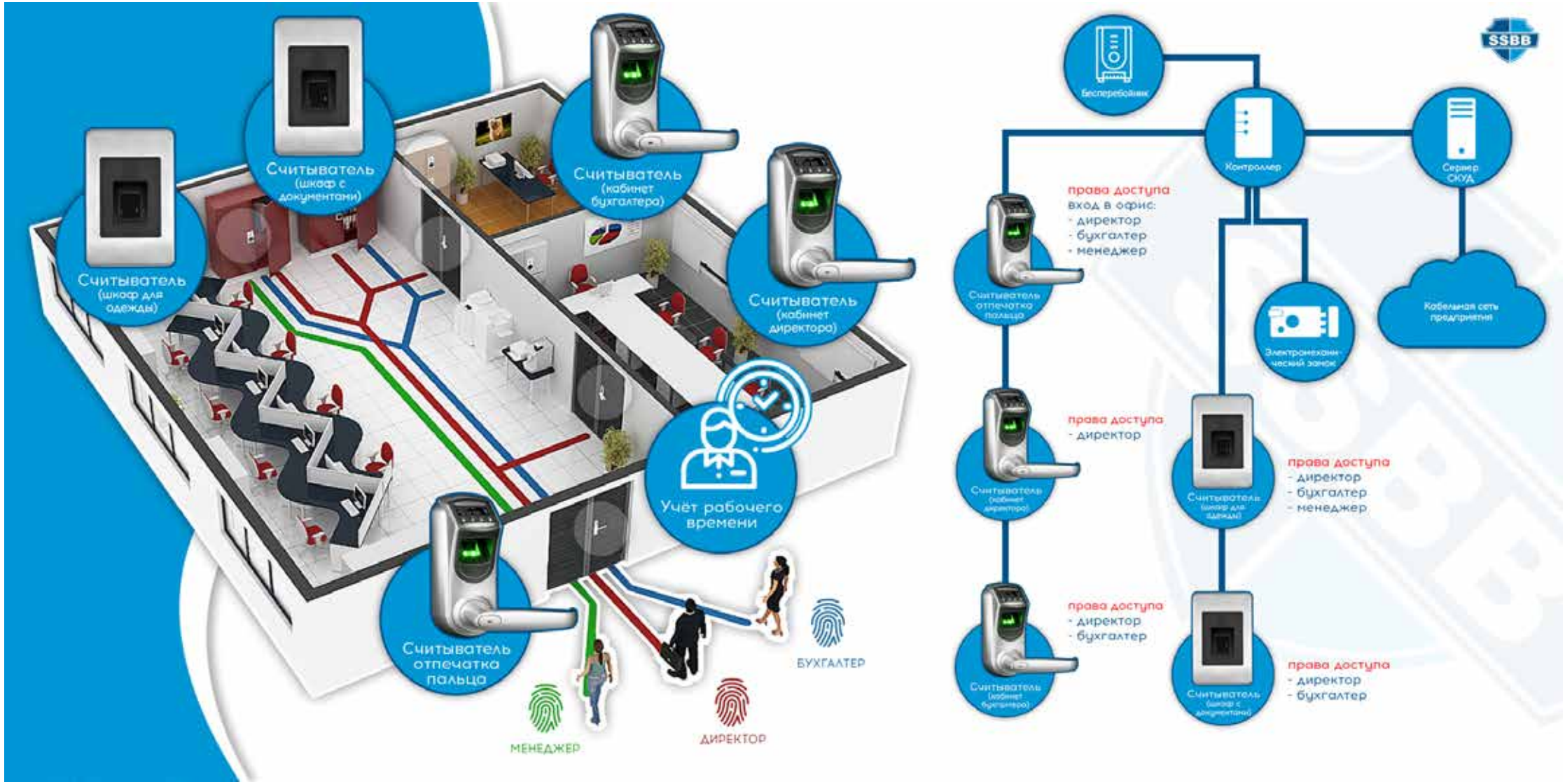
Системы контроля доступа



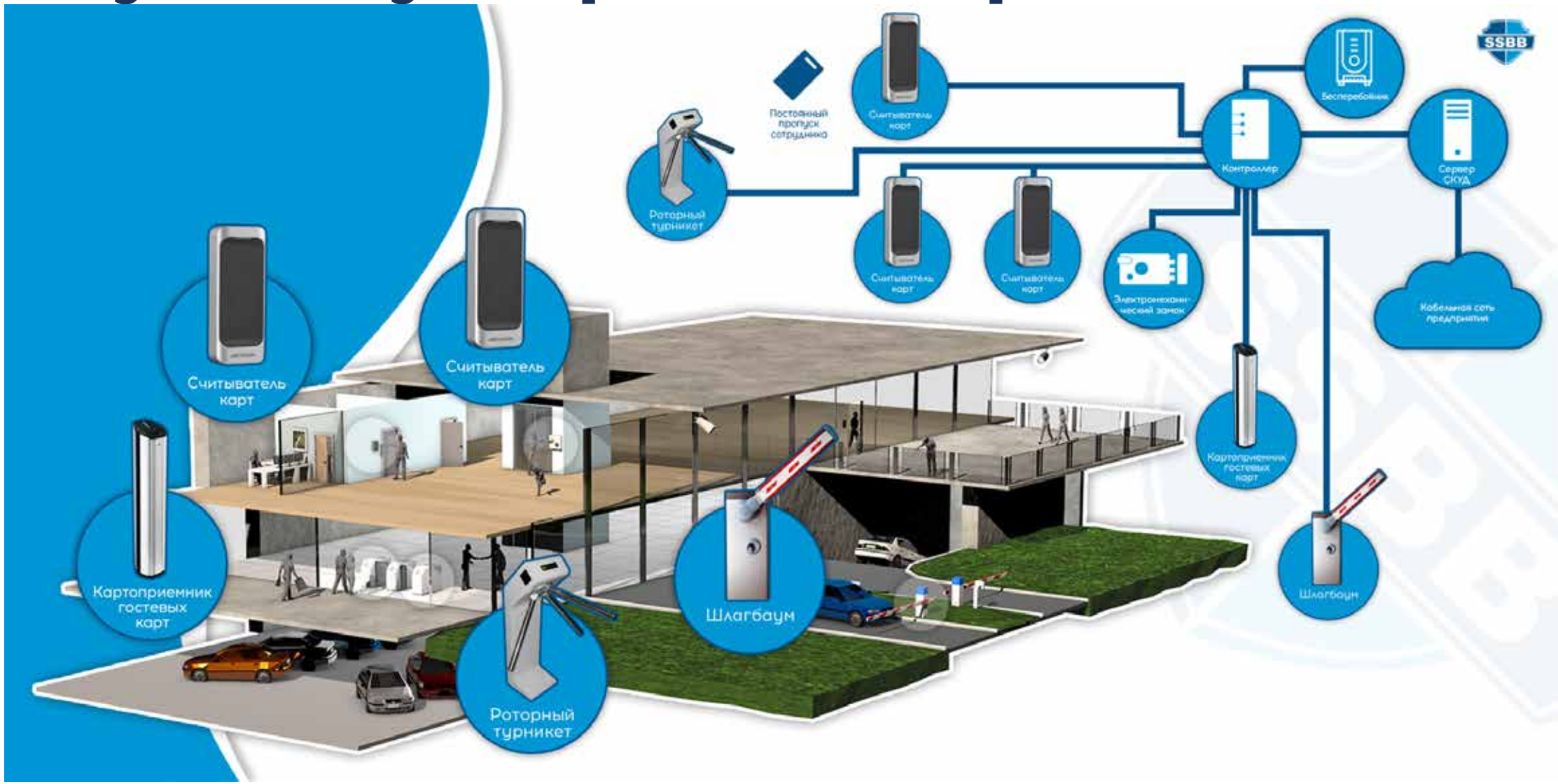
Системы контроля доступа



Биометрическая система управления доступом и учет рабочего времени

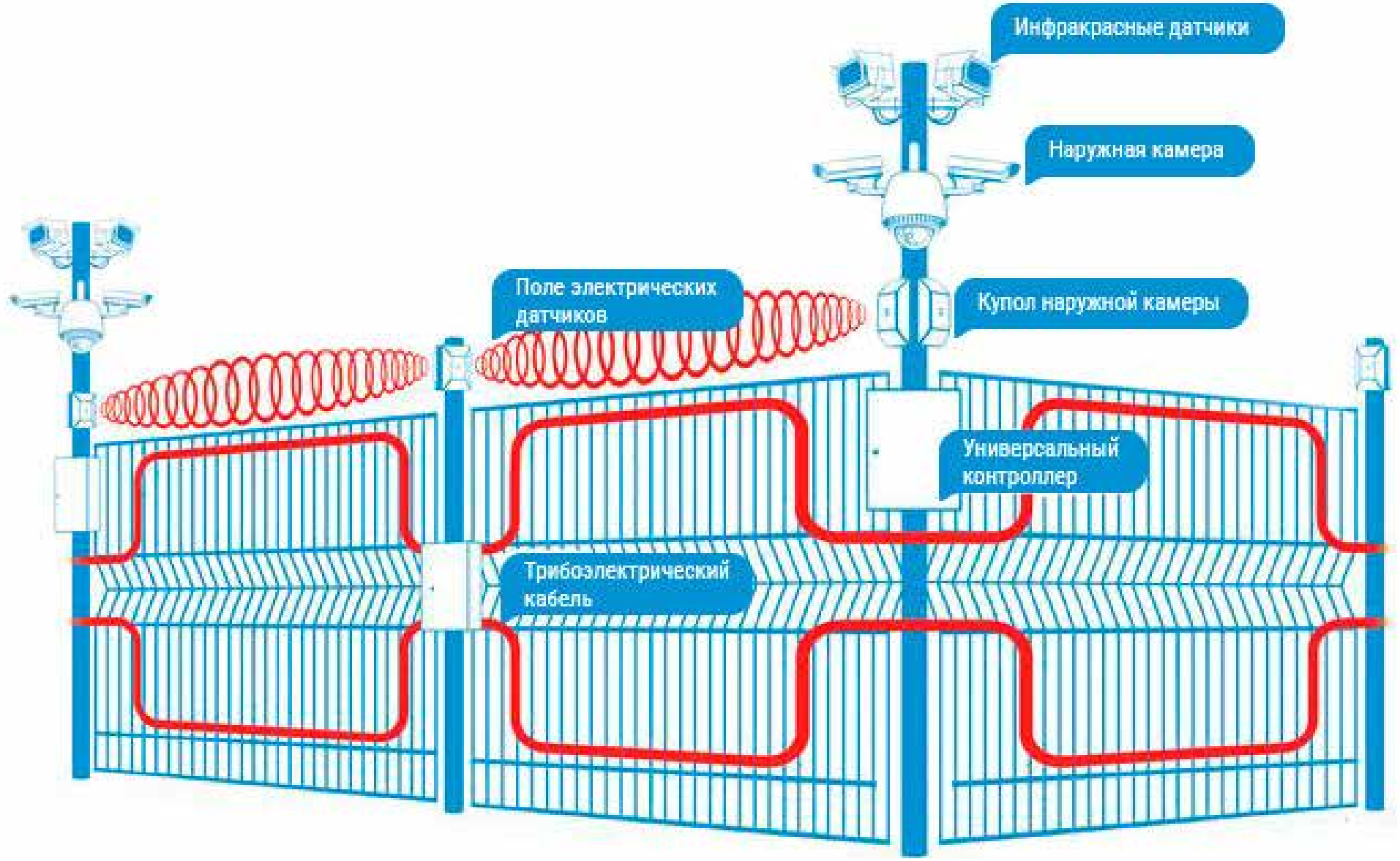


Карточная система контроля и управления доступом и учет рабочего времени



Системы охраны периметра

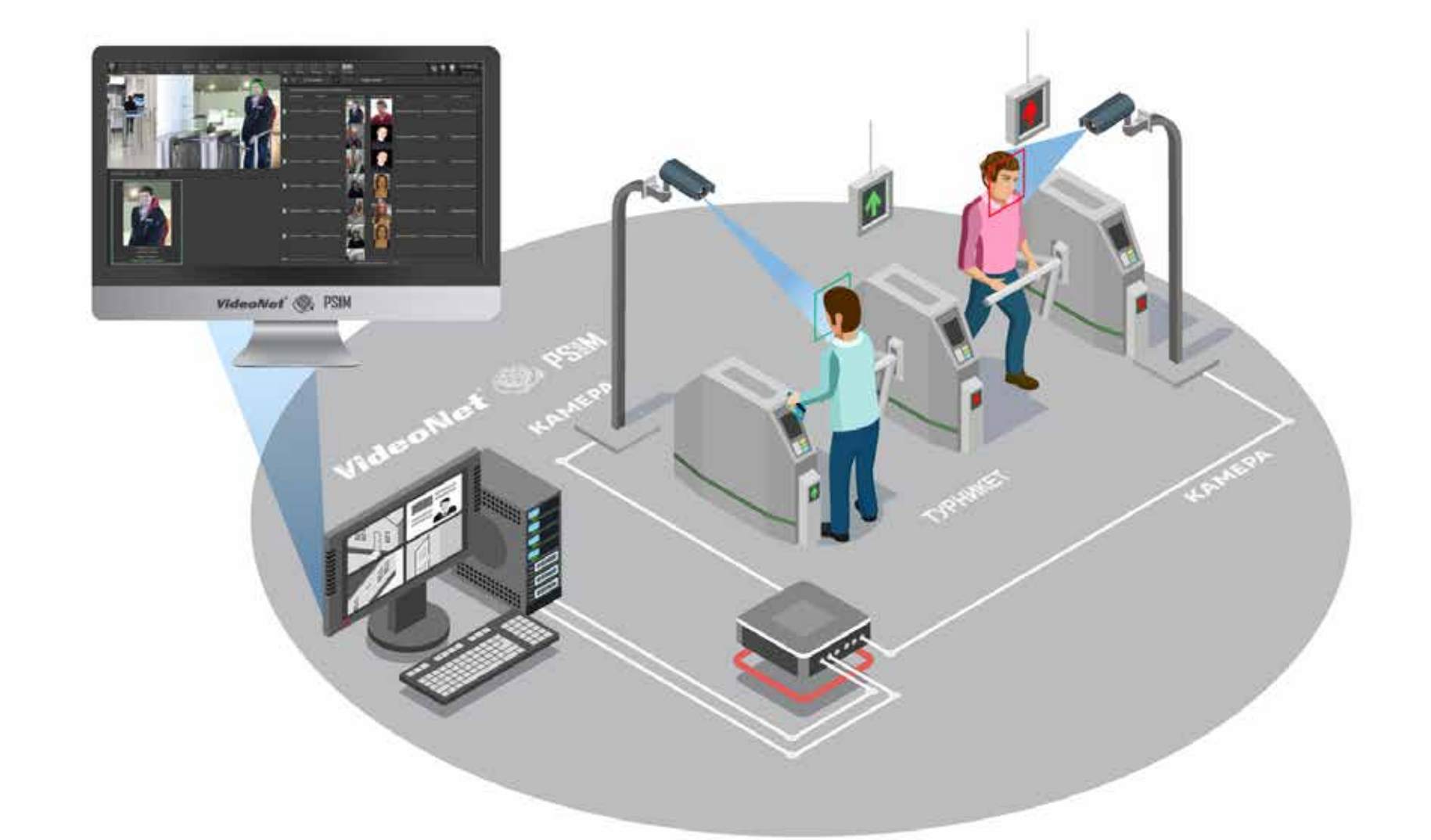
Системы охраны периметра



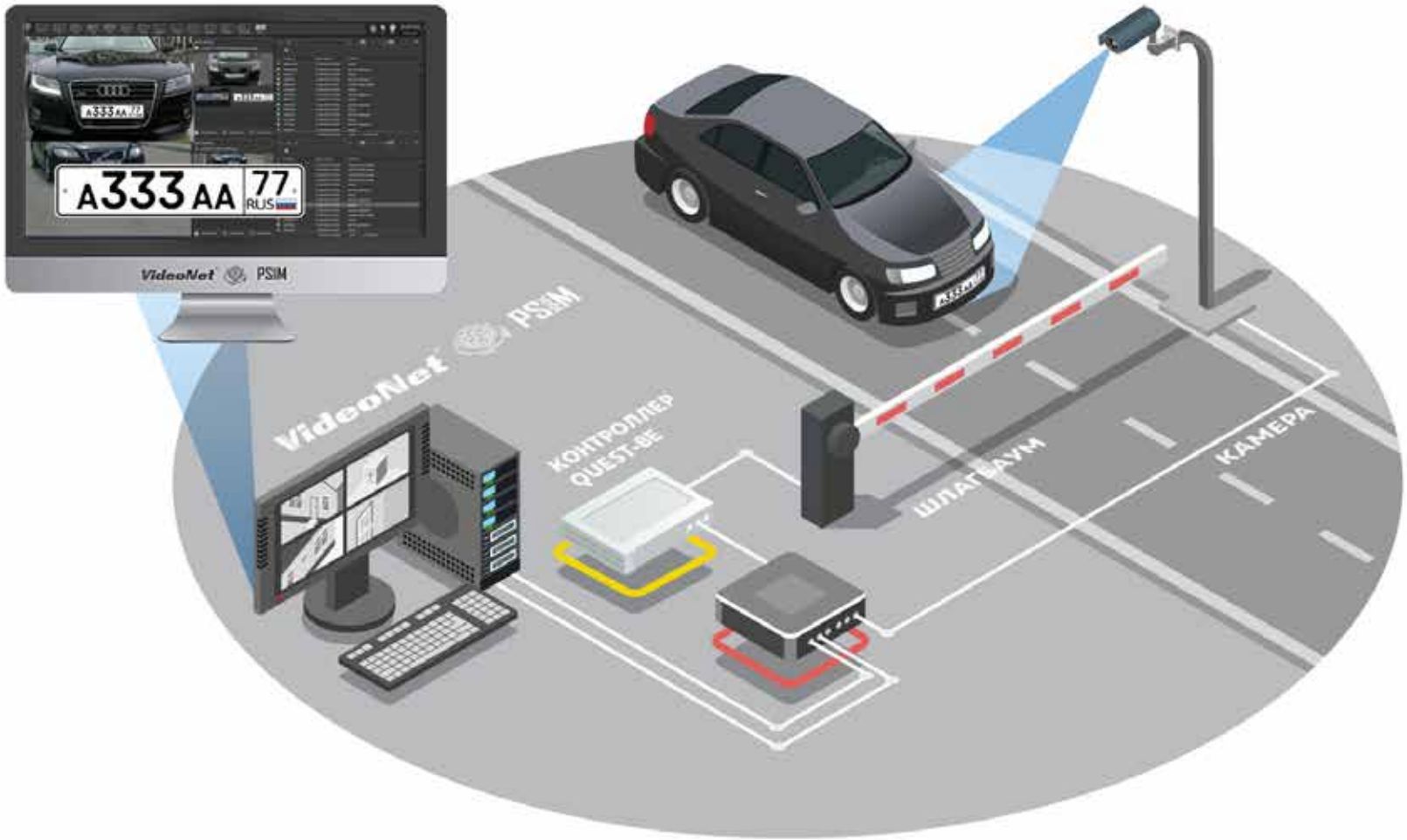
Состав электронных средств охраны

Системы видеонаблюдения

Системы видеонаблюдения
Системы контроля доступа



Системы видеонаблюдения
Системы контроля доступа

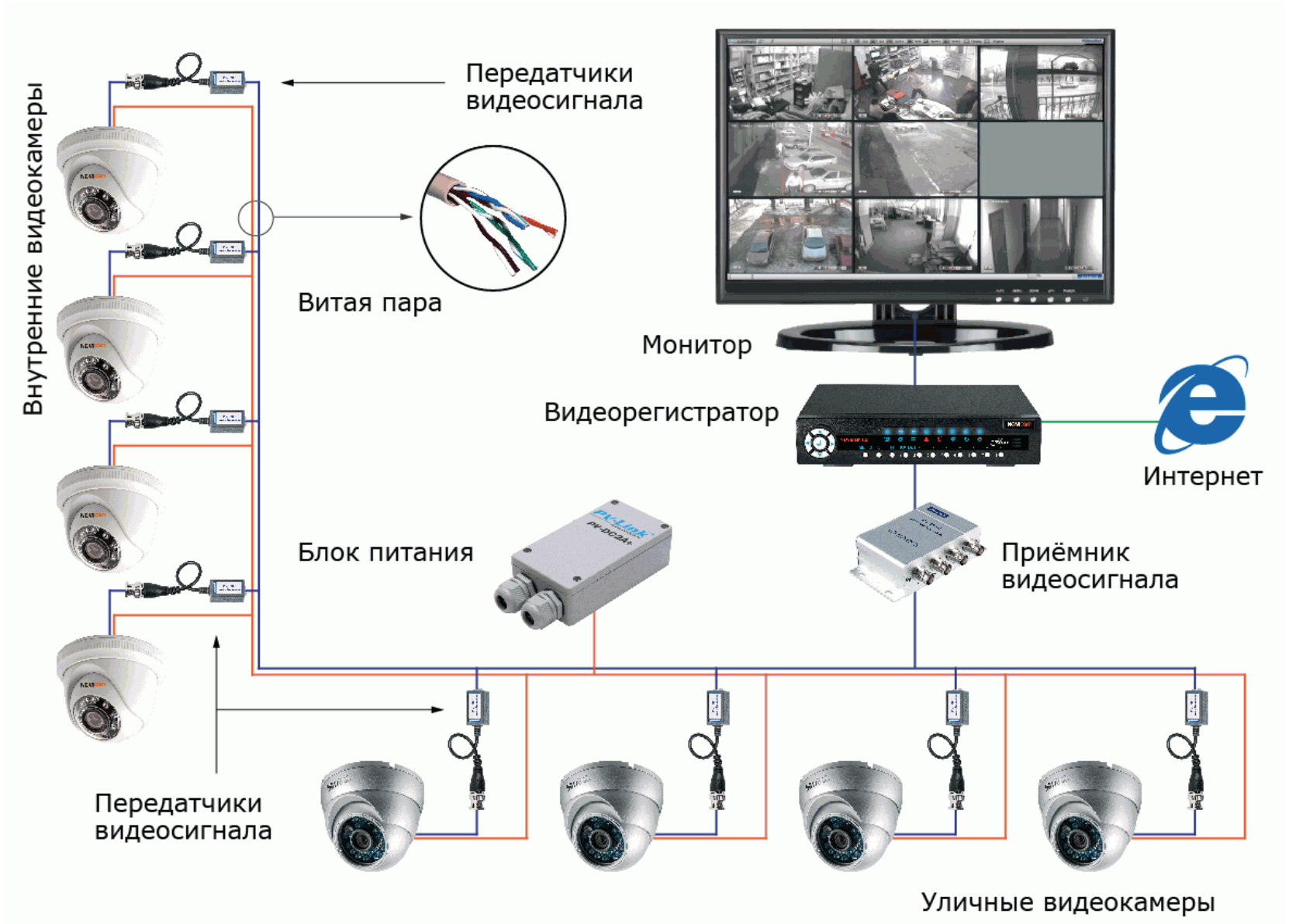


Системы видеонаблюдения

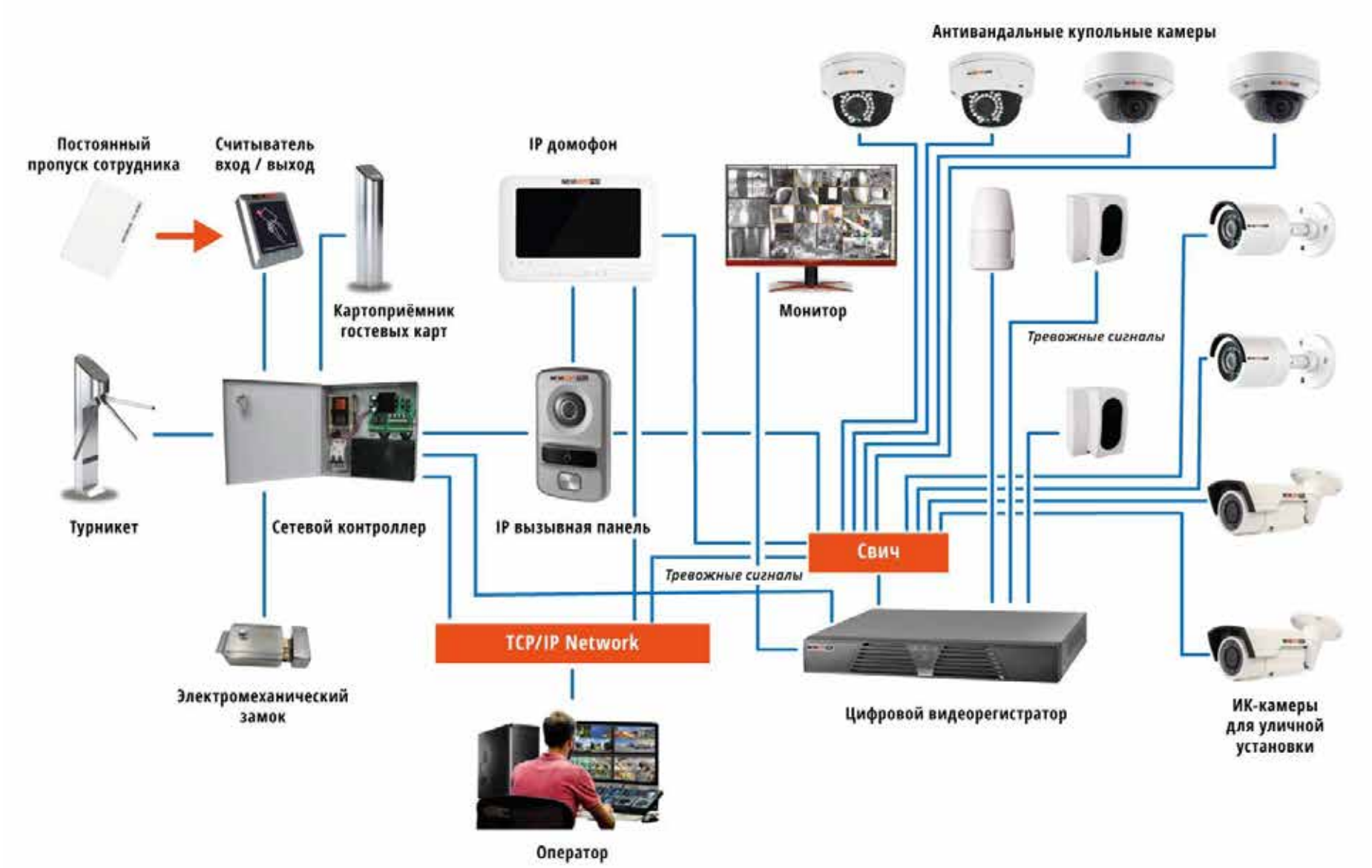
Системы видеонаблюдения

Системы видеонаблюдения

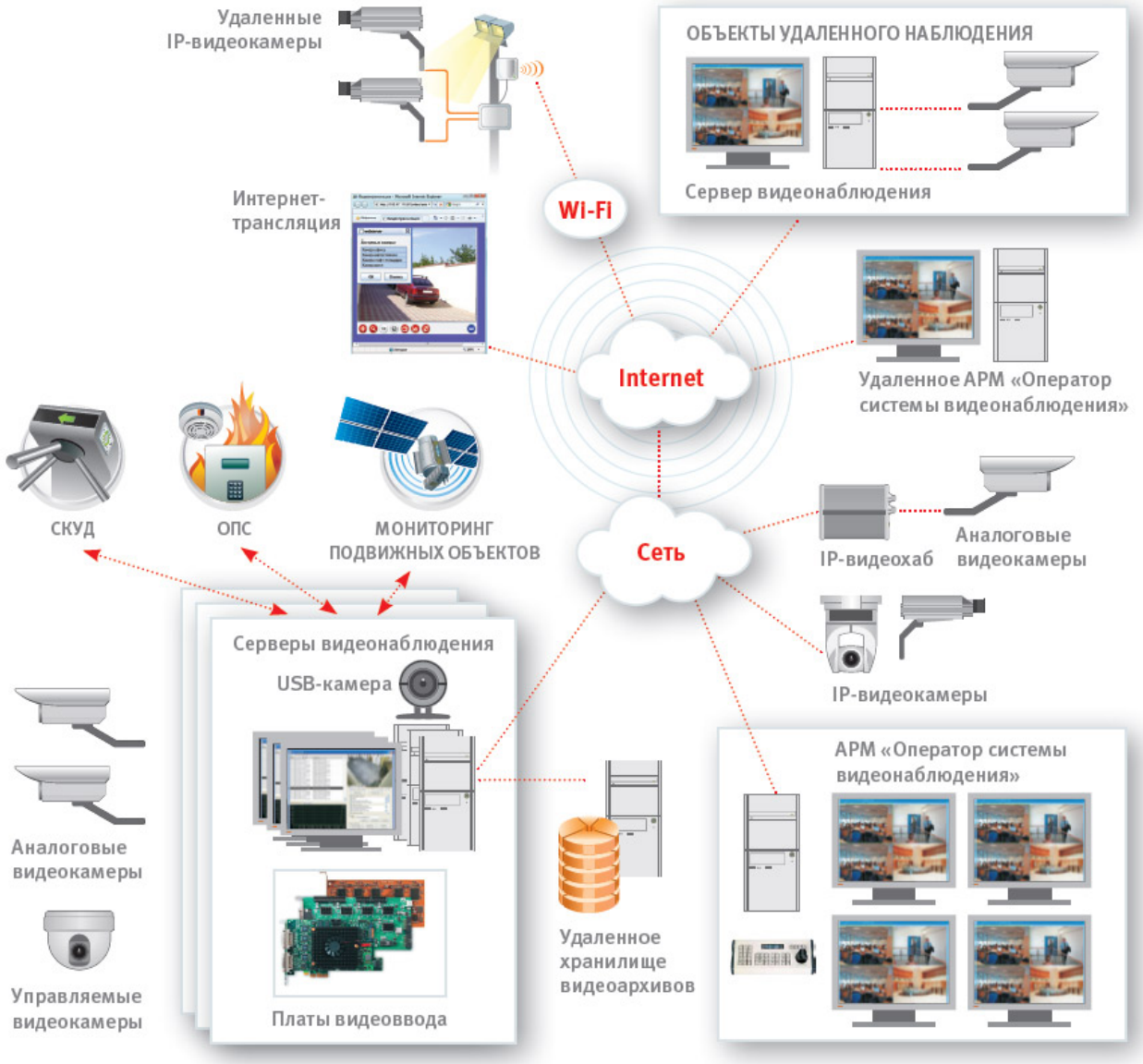
Системы видеонаблюдения



Системы видеонаблюдения



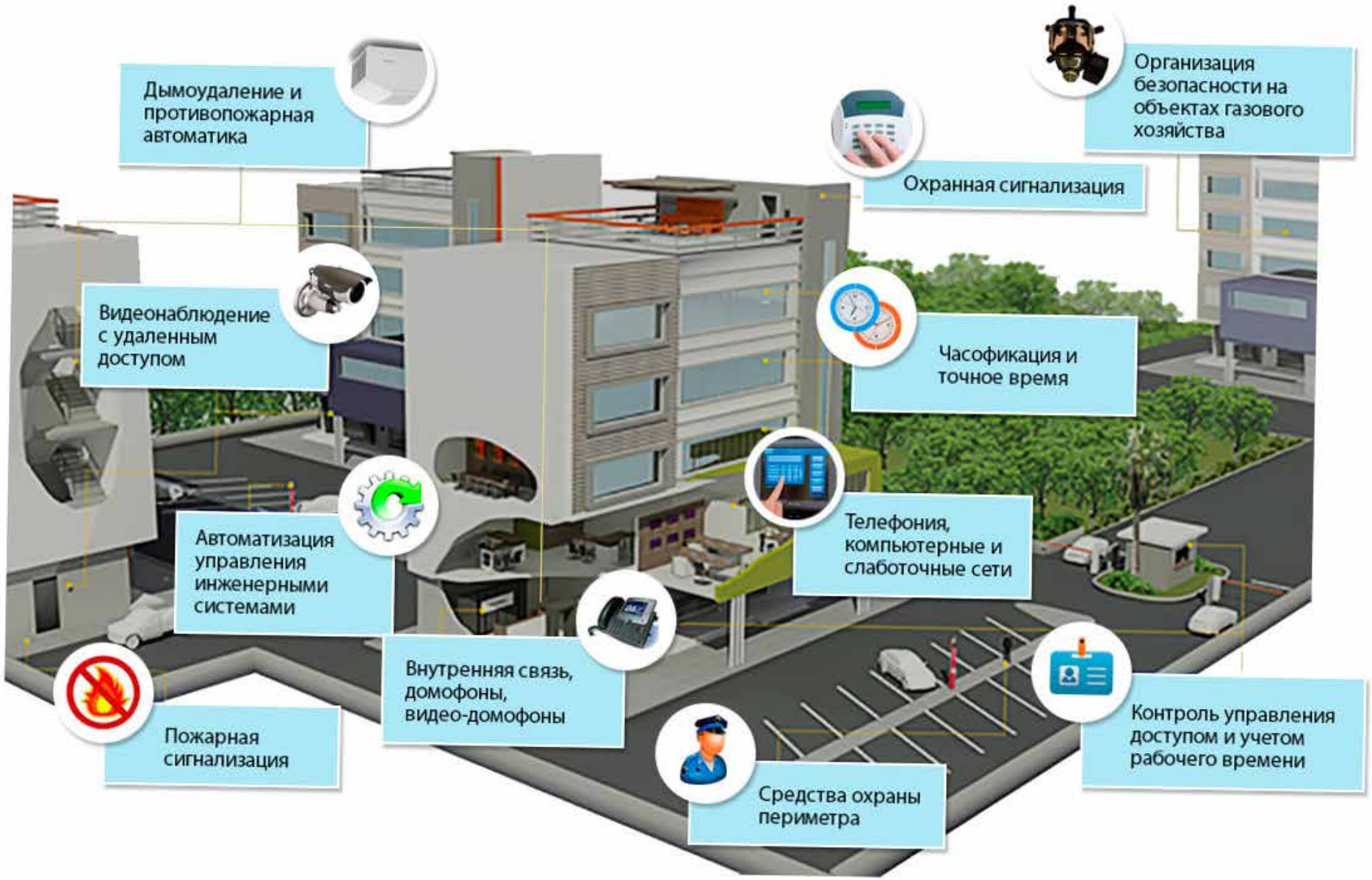
Системы видеонаблюдения



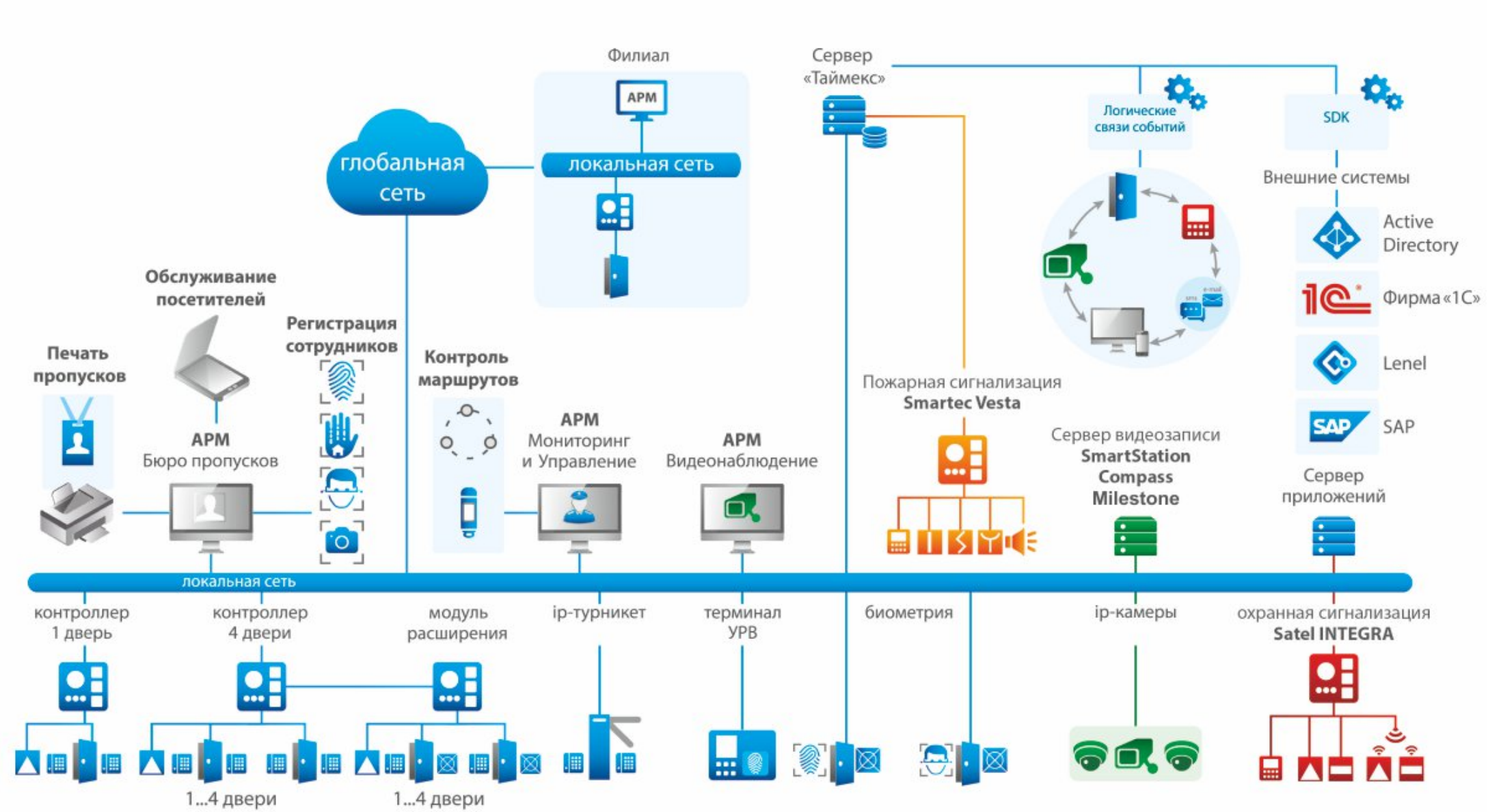
Системы видеонаблюдения

Системы контроля

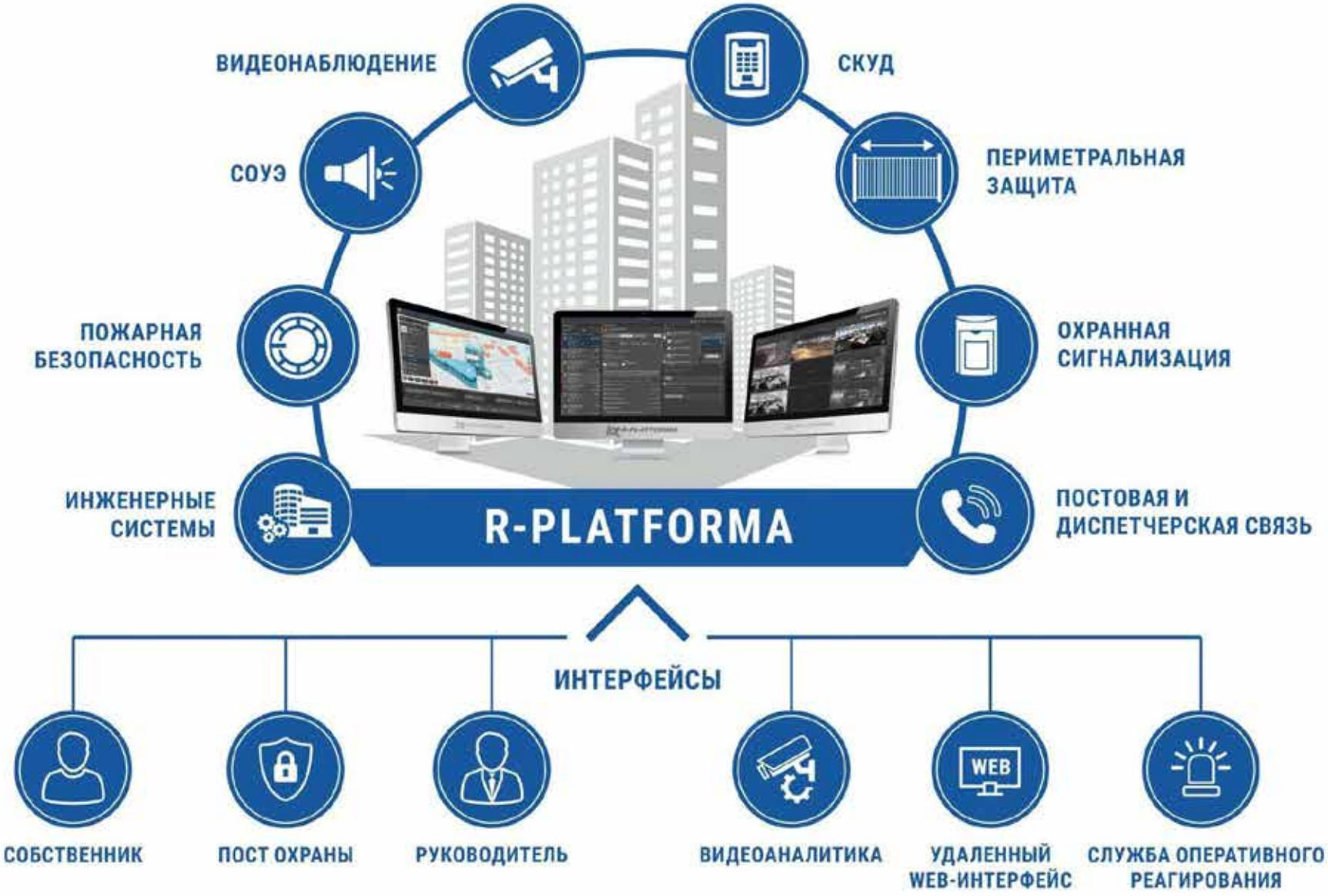
Комплексные системы безопасности и контроля

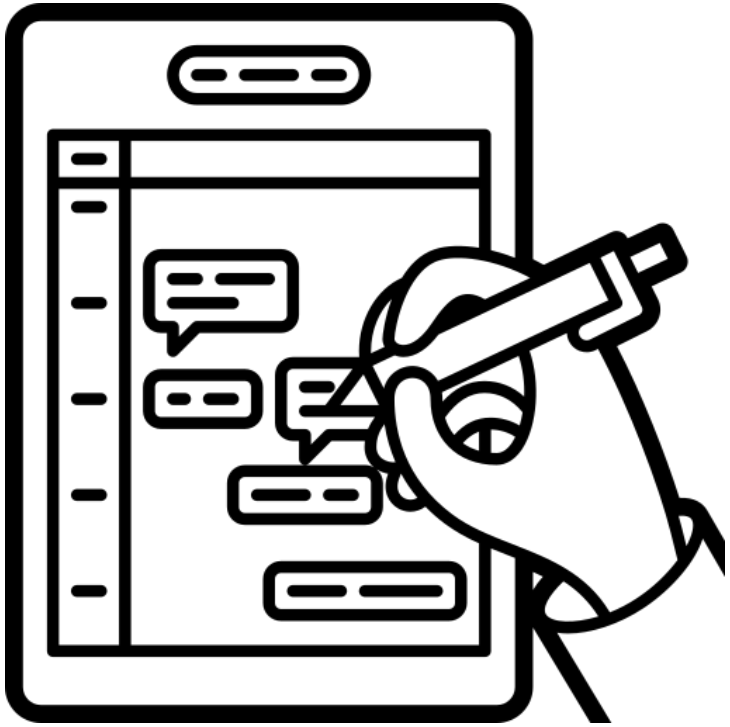


Комплексные системы безопасности и контроля



Комплексные системы безопасности и контроля





4. Политика безопасности предприятия (организации)

Политика безопасности

- **Политика безопасности определяет стратегию управления в области информационной безопасности**, а также меру внимания и количество ресурсов, которые считает целесообразным выделить руководство.
- **Политика безопасности строится на основе анализа рисков, которые признаются реальными для ИС организации**. Когда проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. и.

Политика безопасности

- В терминах компьютерной безопасности **политику можно определить как изданный документ (или свод документов),** в котором рассмотрены вопросы философии, организации, стратегии, методов в отношении конфиденциальности, целостности и пригодности информации и информационных систем.
- Таким образом, политика безопасности информационных объектов – **это совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов**.

Политика безопасности

- **Задача ПБ состоит в том, чтобы сформулировать цели политики информационной безопасности и обеспечить ее поддержку руководством организации.**
- Администрация должна поставить четкую цель и оказывать всестороннюю поддержку ИБ посредством распространения политики безопасности среди сотрудников организации
- Целесообразность выбора любого из средств управления ИБ должна определяться в свете конкретных рисков, присущих организации.

Политика безопасности

- **Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа** высокоуровневой политики, поддерживаемого конкретными документами специализированных политик и процедур безопасности.
- Высокоуровневая политика безопасности должна периодически пересматриваться, гарантируя тем самым учет текущих потребностей организации.

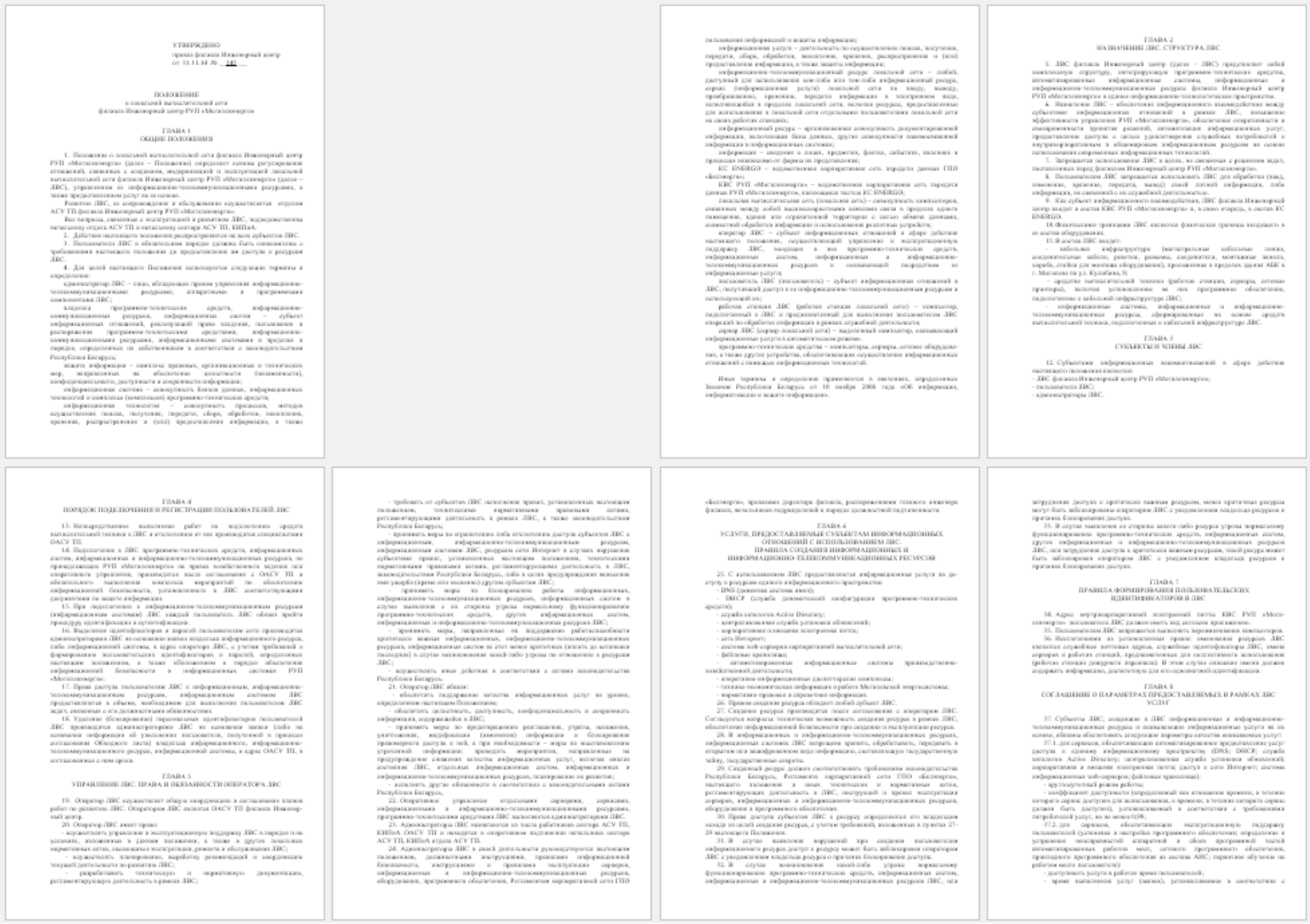
Основные требования к политике безопасности

- Политика безопасности должна быть:
  - а) реалистичной,
  - б) выполнимой,
  - в) краткой,
  - г) понятной,
  - д) не приводить к существенному снижению общей производительности бизнес-подразделений компании.

Политика безопасности

- Документация по политике информационной безопасности предприятия может включать в себя следующие **разделы**:
  - 1. Общие положения
  - 2. Политика управления паролями
  - 3. Идентификация пользователей
  - 4. Полномочия пользователей
  - 5. Защита информационных ресурсов ИС от компьютерных вирусов
  - 6. Правила установки и контроля сетевых соединений
  - 7. Правила политики безопасности по работе с системой электронной почты
  - 8. Правила обеспечения безопасности информационных ресурсов

Пример политики информационной безопасности



УТВЕРЖДЕНО
приказ филиала Инженерный центр
от 11.11.14 № 145

ПОЛОЖЕНИЕ
о локальной вычислительной сети
филиала Инженерный центр РУП «Мистиллоинтерпо»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Положение о локальной вычислительной сети филиала Инженерный центр РУП «Мистиллоинтерпо» (далее – Положение) определяет основы регулирования отношений, связанных с созданием, эксплуатацией и модернизацией локальной вычислительной сети филиала Инженерный центр РУП «Мистиллоинтерпо» (далее – ЛВС), управлением ее информационно-телекоммуникационными ресурсами, а также предоставлением услуг на ее основе.

Развитие ЛВС, ее сопровождение и обслуживание осуществляется отделом АСУ ТП филиала Инженерный центр РУП «Мистиллоинтерпо».

Все вопросы, связанные с эксплуатацией и развитием ЛВС, подлежат согласованию с отделом АСУ ТП и начальником центра АСУ ТП, ИПиА.

2. Действие настоящего положения распространяется на всех субъектов ЛВС.

3. Подключаемая ЛВС к обязательным нормам должна быть соответствовать с требованиями настоящего положения до предоставления им доступа к ресурсам ЛВС.

4. Для целей настоящего Положения используются следующие термины и определения:

администратор ЛВС – лицо, обладающее правами управления информационно-телекоммуникационными ресурсами, осуществляющее и программными комплексами ЛВС;

владелец программно-технических средств, информационно-коммуникационных ресурсов, информационных систем – субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационно-коммуникационными ресурсами, информационными системами в пределах и порядке, определенных их собственником в соответствии с законодательством Республики Беларусь;

защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации;

информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также

ГЛАВА 2
НАЗНАЧЕНИЕ ЛВС. СТРУКТУРА ЛВС

5. ЛВС филиала Инженерный центр (далее – ЛВС) представляет собой комплексную структуру, интегрирующую программно-технические средства, автоматизированные информационные системы, информационные и информационно-телекоммуникационные ресурсы филиала Инженерный центр РУП «Мистиллоинтерпо» в единое информационно-технологическое пространство.

6. Назначение ЛВС – обеспечение информационного взаимодействия между субъектами информационных отношений в рамках ЛВС, повышение эффективности управления РУП «Мистиллоинтерпо», обеспечение сохранности и своевременности принятия решений, автоматизация информационных услуг, предоставление доступа с целью удовлетворения служебных потребностей к внутрикорпоративным и общемировым информационным ресурсам на основе использования современных информационных технологий.

7. Запрещается использование ЛВС в целях, не связанных с решением задач, поставленных перед филиалом Инженерный центр РУП «Мистиллоинтерпо».

8. Пользователям ЛВС запрещается использовать ЛВС для обработки (хранения, изменения, принятия, передачи, выноса) иной личной информации, либо информации, не связанной с их служебной деятельностью.

9. Как субъект информационного взаимодействия, ЛВС филиала Инженерный центр входит в состав ЕИС РУП «Мистиллоинтерпо» и, в свою очередь, в состав ЕС ЭНЕРГО.

10. Физическими границами ЛВС являются физические границы входящего в ее состав оборудования.

11. В состав ЛВС входят:

- кабельная инфраструктура (магистральные кабельные линии, соединительные кабели, розетки, разъемы, соединители, монтажные шкафы, короба, стойки для монтажа оборудования), проложенная в пределах здания АБК в г. Мистиллоинтерпо по ул. Кулибина, 9;
- средства вычислительной техники (рабочие станции, серверы, активные принтеры), включая установленное на них программное обеспечение, подключенное к кабельной инфраструктуре ЛВС;
- информационные системы, информационные и информационно-телекоммуникационные ресурсы, сформированные на основе средств вычислительной техники, подключенных к кабельной инфраструктуре ЛВС.

ГЛАВА 3
СУБЪЕКТЫ И ЧЛЕНЫ ЛВС

12. Субъектами информационных взаимоотношений в сфере действия настоящего положения являются:
- ЛВС филиала Инженерный центр РУП «Мистиллоинтерпо»;
- пользователи ЛВС;
- администраторы ЛВС.

ГЛАВА 4
ПОРЯДОК ПОДКЛЮЧЕНИЯ И РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ ЛВС

13. Непосредственное выполнение работ по подключению средств вычислительной техники к ЛВС и отключению от них производится специалистами ОАСУ ТП.

14. Подключение к ЛВС программно-технических средств, информационных систем, информационных и информационно-телекоммуникационных ресурсов, не принадлежащих РУП «Мистиллоинтерпо» на правах хозяйственного ведения или оперативного управления, производится после согласования с ОАСУ ТП и обязательного выполнения комплекса мероприятий по обеспечению информационной безопасности, установленного в ЛВС соответствующими документами по защите информации.

15. При подключении к информационно-телекоммуникационным ресурсам (информационным системам) ЛВС каждый пользователь ЛВС обязан пройти процедуру идентификации и аутентификации.

16. Выделение идентификаторов и паролей пользователям сети производится администратором ЛВС по согласованию с владельцами информационного ресурса, либо информационной системы, в ходе которого ЛВС, с учетом требований к формированию возможностей идентификаторов и паролей, определенных настоящим положением, а также обязанностями и порядок обеспечения информационной безопасности в информационных системах РУП «Мистиллоинтерпо».

17. Права доступа пользователя ЛВС к информационным, информационно-телекоммуникационным ресурсам, информационным системам ЛВС предоставляются в объеме, необходимом для выполнения пользователем ЛВС задач, связанных с его должностными обязанностями.

18. Удаление (блокирование) учетных записей идентификаторов пользователей ЛВС производится администратором ЛВС по заявочным запискам (либо на основании информации об увольнении пользователя, полученной в приказе о согласовании Обходного листа) владельцев информационного, информационно-телекоммуникационного ресурсов, информационной системы, в ходе ОАСУ ТП, в согласованные с ним сроки.

ГЛАВА 5
УПРАВЛЕНИЕ ЛВС. ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА ЛВС

19. Оператор ЛВС осуществляет обзоры соединений и согласованных взаимодействий работ по развитию ЛВС. Оператором ЛВС является ОАСУ ТП филиала Инженерный центр.

20. Оператор ЛВС имеет право:

- осуществлять управление и эксплуатационную поддержку ЛВС в пределах и на условиях, изложенных в данном положении, а также в других локальных нормативных актах, касающихся конструкции, ремонта и обслуживания ЛВС;
- осуществлять планирование, разработку рекомендаций и координацию текущей деятельности по развитию ЛВС;
- разрабатывать технологию и нормативную документацию, регламентирующую деятельность в рамках ЛВС;

- требовать от субъектов ЛВС выполнения правил, установленных настоящим положением, технологическими нормативными правовыми актами, регламентирующими деятельность в рамках ЛВС, а также законодательством Республики Беларусь;
- применять меры по ограничению либо отключению доступа субъектов ЛВС к информационным, информационно-телекоммуникационным ресурсам, информационным системам ЛВС, ресурсам сети Интернет в случаях нарушения субъектами правил, установленных настоящим положением, технологическими нормативными правовыми актами, регламентирующими деятельность в ЛВС, законодательством Республики Беларусь, либо в целях предупреждения нанесения ими ущерба (прямо или косвенно) другим субъектам ЛВС;
- применять меры по бесперебойной работы информационных, информационно-телекоммуникационных ресурсов, информационных систем в случае выявления в их отношении угрозы нормальному функционированию программно-технических средств, других информационных систем, информационных и информационно-телекоммуникационных ресурсов ЛВС;
- применять меры, направленные на поддержание работоспособности критически важных информационных, информационно-телекоммуникационных ресурсов, информационных систем не этот менее критических (исключительно в отношении последних) в случае возникновения какой-либо угрозы по отношению к ресурсам ЛВС;
- осуществлять иные действия в соответствии с актами законодательства Республики Беларусь.

21. Оператор ЛВС обязан:

- обеспечивать поддержание качества информационных услуг на уровне, определенном настоящим Положением;
- обеспечивать сохранность, доступность, конфиденциальность и сохранность информации, содержащейся в ЛВС;
- принимать меры по предупреждению расплавления, утраты, искажения, уничтожения, модификации (изменения) информации и блокированию противоправного доступа к ней, а при необходимости – меры по восстановлению утраченной информации; проводить мероприятия, направленные на предупреждение сложных качества информационных услуг, могущих нанести изменения ЛВС, отдельным информационным системам, информационным и информационно-телекоммуникационным ресурсам, планированию их развития;
- выполнять другие обязанности в соответствии с законодательством актами Республики Беларусь.

22. Оперативное управление отдельными серверами, сервисами, информационными и информационно-телекоммуникационными ресурсами, программно-техническими средствами ЛВС выполняется администраторами ЛВС.

23. Администраторы ЛВС назначаются из числа работников сектора АСУ ТП, КИПиА ОАСУ ТП и находятся в оперативном подчинении начальника сектора АСУ ТП, КИПиА отдела АСУ ТП.

24. Администраторы ЛВС в своей деятельности руководствуются настоящим положением, должностными инструкциями, приказами информационной безопасности, инструкциями и правилами эксплуатации серверов, информационных и информационно-телекоммуникационных ресурсов, оборудования, программного обеспечения, Регламентом корпоративной сети ГПО «Белэнерго», приказами директора филиала, распоряжениями главного инженера филиала, начальников подразделений и порядке должностной подчиненности.

ГЛАВА 6
УСЛУГИ, ПРЕДОСТАВЛЯЕМЫЕ СУБЪЕКТАМ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ С ИСПОЛЬЗОВАНИЕМ ЛВС. ПРАВИЛА СОЗДАНИЯ ИНФОРМАЦИОННЫХ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ РЕСУРСОВ

25. С использованием ЛВС предоставляются информационные услуги по доступу к ресурсам единого информационного пространства:
- DNS (доменная система имен);
- DHCP (служба динамической конфигурации программно-технических средств);
- служба каталогов Active Directory;
- контроллеров и доменов электронная почта;
- корпоративная и внешняя электронная почта;
- сеть Интернет;
- система web-серверов корпоративной вычислительной сети;
- файловые ресурсы;
- автоматизированные информационные системы производственно-хозяйственной деятельности;
- юридическая информационная диалоговую систему комплекса;
- технико-экономическая информация о работе Мистиллоинтерпо системы;
- нормативно-правовая и справочная информация.

26. Правом создания ресурсов обладает любой субъект ЛВС.

27. Созданные ресурсы производятся после согласования с оператором ЛВС. Согласуются вопросы технической возможности создания ресурсов в рамках ЛВС, обеспечения информационной безопасности при создании и эксплуатации ресурсов.

28. В информационных и информационно-телекоммуникационных ресурсах, информационных системах ЛВС запрещено хранить, обрабатывать, передавать в открытом виде информацию иного информации, составляющую государственную тайну, государственные секреты.

29. Созданный ресурс должен соответствовать требованиям законодательства Республики Беларусь, Регламенту корпоративной сети ГПО «Белэнерго», настоящего положения и иных технических и нормативных актов, регламентирующих деятельность в ЛВС, инструкций и правил эксплуатации серверов, информационных и информационно-телекоммуникационных ресурсов, оборудования и программного обеспечения.

30. Права доступа субъектов ЛВС к ресурсу определяются его владельцем исходя из целей создания ресурса, с учетом требований, изложенных в пунктах 27-29 настоящего Положения.

31. В случае выявления нарушений при создании пользователем информационного ресурса доступ к ресурсу может быть заблокирован оператором ЛВС с уведомлением владельца ресурса о причинах блокирования доступа.

32. В случае возникновения какой-либо угрозы нормальному функционированию программно-технических средств, информационных систем, информационных и информационно-телекоммуникационных ресурсов ЛВС, или

ГЛАВА 7
ПРАВИЛА ФОРМИРОВАНИЯ ПОЛЬЗОВАТЕЛЬСКИХ ИДЕНТИФИКАТОРОВ В ЛВС

34. Адрес зарегистрированной электронной почты ЕИС РУП «Мистиллоинтерпо» пользователя ЛВС должен иметь вид согласно приложению.

35. Пользователям ЛВС запрещается выполнять переименование компьютеров.

36. Пользователям из установленных правил именования ресурсов ЛВС являются служебные почтовые адреса, служебные идентификаторы ЛВС, имена ресурсов и рабочих станций, предназначенных для коллективного использования (рабочие станции дежурного персонала). В этом случае описание имени должно содержать информацию, достаточную для его однозначной идентификации.

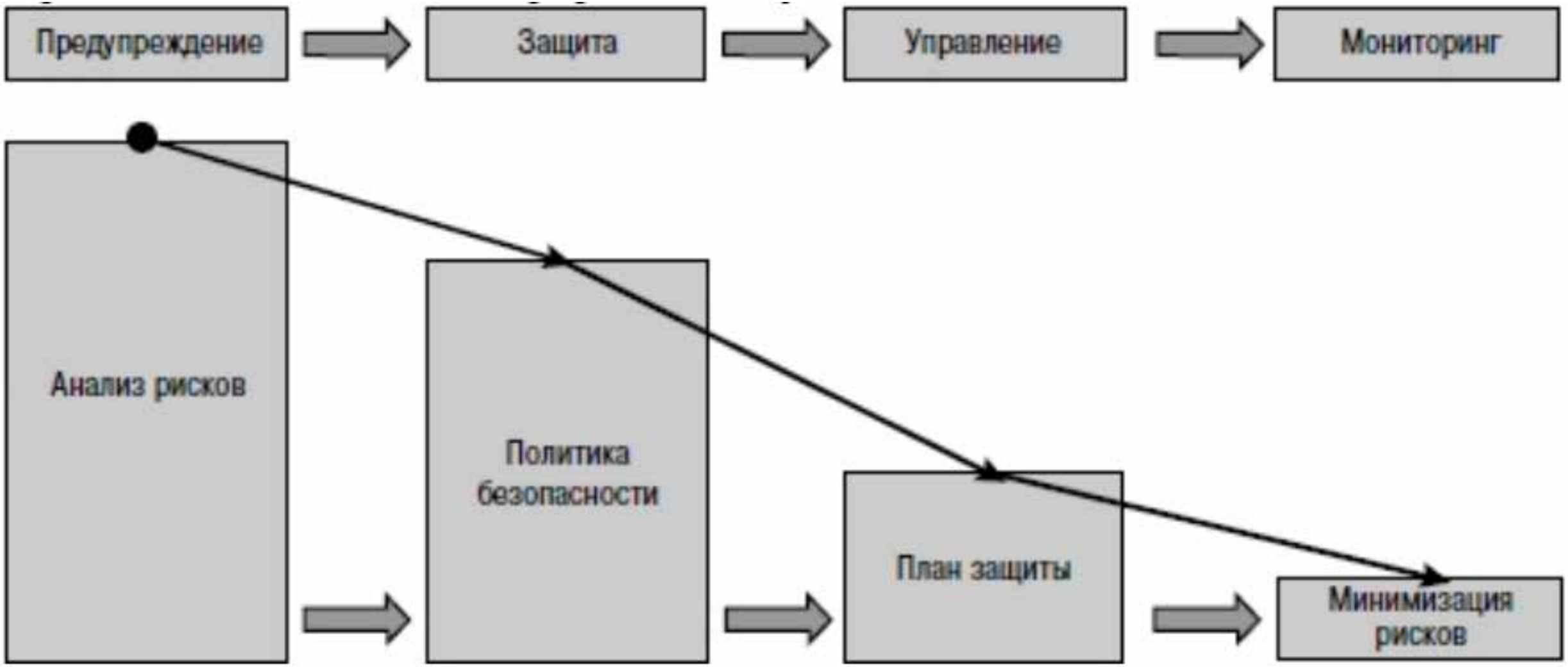
ГЛАВА 8
СОГЛАШЕНИЯ О ПАРАМЕТРАХ ПРЕДОСТАВЛЯЕМЫХ В РАМКАХ ЛВС УСЛУГ

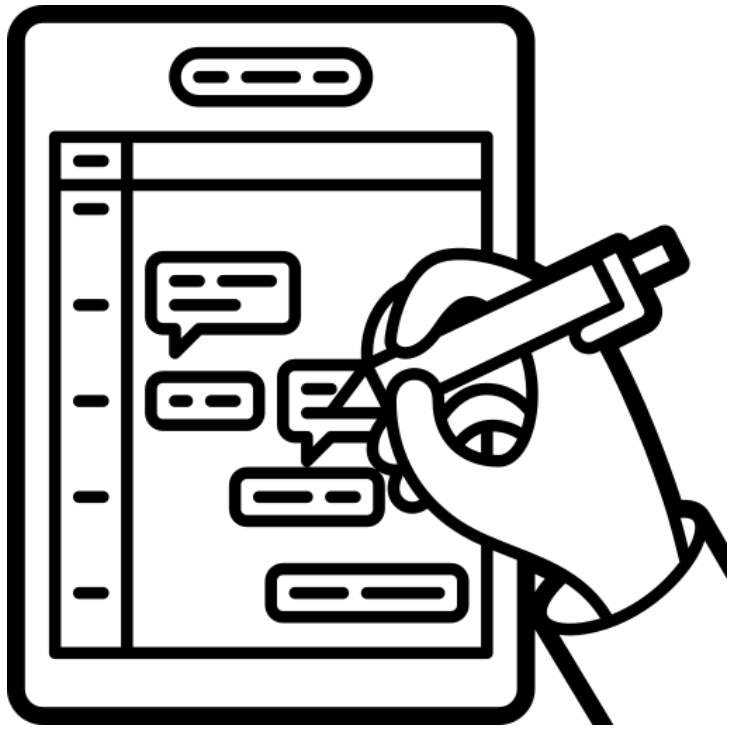
37. Субъекты ЛВС, создавая в ЛВС информационные и информационно-телекоммуникационные ресурсы и оказывая информационные услуги на их основе, обязаны обеспечивать следующие параметры качества оказываемых услуг:

37.1. для сервисов, обеспечивающих автоматизированное предоставление услуг доступа к единому информационному пространству (DNS; DHCP; служба каталогов Active Directory; централизованная служба установки обновлений корпоративная и внешняя электронная почта; доступ к сети Интернет; система информационных web-серверов; файловые хранилища):
- круглосуточный режим работы;
- коэффициент доступности (определенный как отношение времени, в течение которого сервис доступен для использования, к времени, в течение которого сервис должен быть доступен), устанавливаемый в соответствии с требованиями потребителей услуг, но не менее 0,98;

37.2. для сервисов, обеспечивающих эксплуатационную поддержку пользователей (установка и настройка программного обеспечения; определение и устранение неисправностей аппаратной и общего программного плана автоматизированных рабочих мест; сетевого программного обеспечения, прикладного программного обеспечения из состава АИС; первичное обучение по работе мест пользователя):
- доступность услуги в рабочее время пользователей;
- время выполнения услуг (заявок), устанавливаемое в соответствии с

Процесс разработки политики безопасности компании





5. Рекомендуемые области разработки политики информационной безопасности

5.1 в Республике Беларусь

Методические рекомендации по обеспечению информационной безопасности в Республике Беларусь. Система менеджмента информационной безопасности

- 1. **Методические рекомендации по обеспечению информационной безопасности разработаны в соответствии с СТБ ISO/IEC 27001-2011** «Информационные технологии. Методы обеспечения безопасности. Система менеджмента информационной безопасности. Требования» **и СТБ ISO/IEC 27002-2012** «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности» **и определяют минимально необходимый перечень требований по созданию и внедрению системы менеджмента информационной безопасности в организации** (далее – СМИБ).
- Перечень требований по созданию и внедрению СМИБ может быть расширен либо обоснованно сокращен с учетом особенностей деятельности конкретной организации.
- 2. Настоящие **методические рекомендации предназначены для использования организациями при разработке локальных нормативных правовых актов, определяющих выбранные правовые, организационные либо технические меры (мероприятия) по обеспечению информационной безопасности**. https://oac.gov.by/public/content/files/files/metod_recomend.docx

Методические рекомендации по обеспечению информационной безопасности в Республике Беларусь. Система менеджмента информационной безопасности

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.
СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ГЛАВА 1
ОБЛАСТЬ ПРИМЕНЕНИЯ

1. Методические рекомендации по обеспечению информационной безопасности (далее – методические рекомендации) разработаны в соответствии с СТБ ISO/IEC 27001-2011 «Информационные технологии. Методы обеспечения безопасности. Система менеджмента информационной безопасности. Требования» (далее – СТБ 27001) и СТБ ISO/IEC 27002-2012 «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности» (далее – СТБ 27002) и определяют минимально необходимый перечень требований по созданию и внедрению системы менеджмента информационной безопасности в организации (далее – СМИБ).

Перечень требований по созданию и внедрению СМИБ может быть расширен либо обоснованно сокращен с учетом особенностей деятельности конкретной организации.

2. Настоящие методические рекомендации предназначены для использования организациями при разработке локальных нормативных правовых актов, определяющих выбранные правовые, организационные либо технические меры (мероприятия) по обеспечению информационной безопасности.

ГЛАВА 2
ЭТАПЫ ВНЕДРЕНИЯ СМИБ

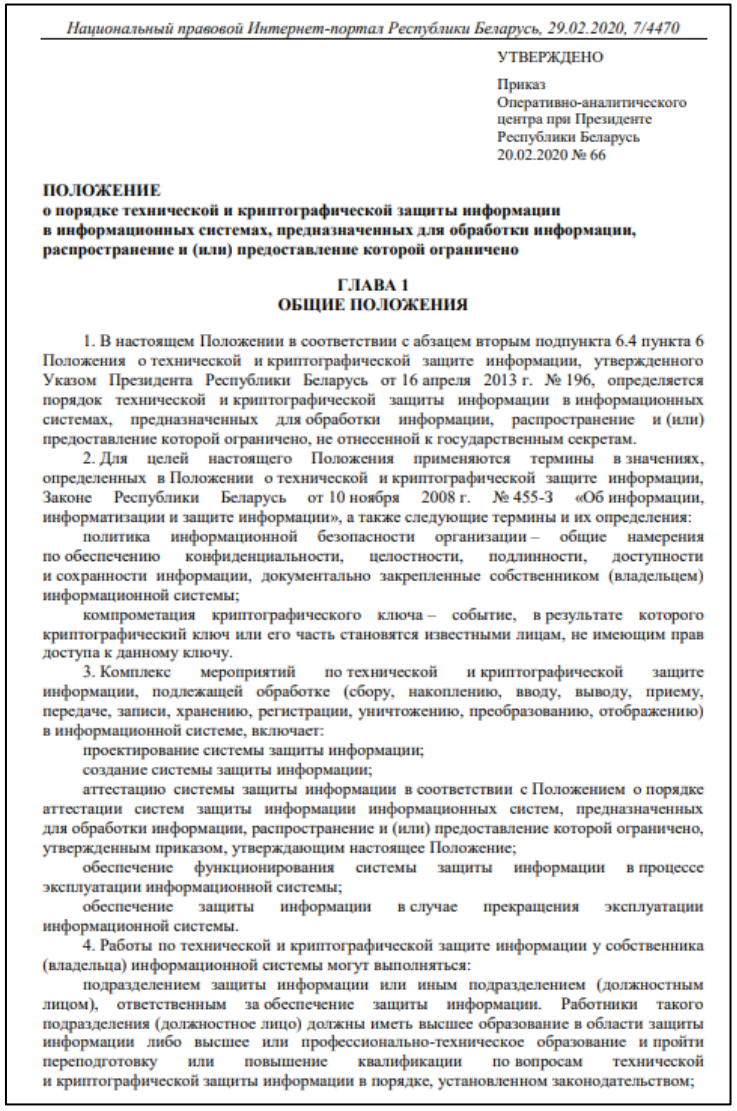
3. На предварительном этапе (до внедрения СМИБ) необходимо определить должностных лиц, ответственных за проведение мероприятий по планированию и дальнейшему внедрению СМИБ в организации.

4. Для эффективного функционирования СМИБ следует использовать непрерывный циклический процесс, который включает в себя следующие этапы:

разработка (планирование);
внедрение (реализация плана);
проверка (анализ эффективности и работоспособности внедренных мер);
совершенствование (устранение обнаруженных недостатков).

- **ГЛАВА 1** Область применения
- **ГЛАВА 2** Этапы внедрения системы менеджмента информационной безопасности в организации (СМИБ)
- **ГЛАВА 3** Разработка (планирование) СМИБ
- **ГЛАВА 4** Внедрение СМИБ
- **ГЛАВА 5** Проверка СМИБ
- **ГЛАВА 6** Совершенствование СМИБ
- **ГЛАВА 7** Требования, предъявляемые К СМИБ
- **ГЛАВА 8** Требования к локальным нормативным правовым актам организации
- **ГЛАВА 9** Требования к организации информационной безопасности
- **ГЛАВА 10** Требования к управлению активами
- **ГЛАВА 11** Требования, связанные с персоналом
- **ГЛАВА 12** Требования к физической защите
- **ГЛАВА 13** Требования к функционированию средств обработки информации, информационных систем и сетей (СОИИСС)
- **ГЛАВА 14** Требования к контролю доступа к СОИИСС
- **ГЛАВА 15** Требования к разработке, внедрению и обслуживанию информационных систем
- **ГЛАВА 16** Требования к управлению инцидентами информационной безопасности
- **ГЛАВА 17** Требования к информационной безопасности при управлении непрерывностью основных процессов организации

ПОЛОЖЕНИЕ о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено



Национальный правовой Интернет-портал Республики Беларусь, 29.02.2020, 7/4470

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
20.02.2020 № 66

ПОЛОЖЕНИЕ
о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. В настоящем Положении в соответствии с абзацем вторым подпункта 6.4 пункта 6 Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, определяется порядок технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

2. Для целей настоящего Положения применяются термины в значениях, определенных в Положении о технической и криптографической защите информации, Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», а также следующие термины и их определения:

политика информационной безопасности организации – общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, документально закрепленные собственником (владельцем) информационной системы;

компрометация криптографического ключа – событие, в результате которого криптографический ключ или его часть становятся известными лицам, не имеющим прав доступа к данному ключу.

3. Комплекс мероприятий по технической и криптографической защите информации, подлежащей обработке (сбору, накоплению, вводу, выводу, приему, передаче, записи, хранению, регистрации, уничтожению, преобразованию, отображению) в информационной системе, включает:

проектирование системы защиты информации;

создание системы защиты информации;

аттестацию системы защиты информации в соответствии с Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом, утверждающим настоящее Положение;

обеспечение функционирования системы защиты информации в процессе эксплуатации информационной системы;

обеспечение защиты информации в случае прекращения эксплуатации информационной системы.

4. Работы по технической и криптографической защите информации у собственника (владельца) информационной системы могут выполняться:

подразделением защиты информации или иным подразделением (должностным лицом), ответственным за обеспечение защиты информации. Работники такого подразделения (должностное лицо) должны иметь высшее образование в области защиты информации либо высшее или профессионально-техническое образование и пройти переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации в порядке, установленном законодательством;

- Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 20.02.2020 № 66
- **ПОЛОЖЕНИЕ о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено**
- https://pravo.by/upload/docs/op/T62004470_1582923600.pdf

ПОЛОЖЕНИЕ о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено

- **ГЛАВА 2 ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ**
- Пункт 8. **На этапе проектирования системы защиты информации осуществляются**:
  - **анализ структуры информационной системы и информационных потоков** (внутренних и внешних) в целях определения состава (количества) и мест размещения элементов информационной системы (аппаратных и программных), ее физических и логических границ;
  - **разработка** (корректировка) политики информационной безопасности организации;
  - **определение требований** к системе защиты информации в техническом задании на создание системы защиты информации (далее - техническое задание);
  - выбор средств технической и криптографической защиты информации;
  - **разработка** (корректировка) общей схемы системы защиты информации.

ПОЛОЖЕНИЕ о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено

- **Пункт 9. Политика информационной безопасности организации должна содержать:**
  - **цели и принципы** защиты информации в организации;
  - **перечень информационных систем**, отнесенных к соответствующим классам типовых информационных систем, а также отдельно стоящих электронных вычислительных машин, используемых в организации и принадлежащих ей на праве собственности или ином законном основании, с указанием подразделения защиты информации или иного подразделения (должностного лица), ответственного за обеспечение защиты информации;
  - **обязанности пользователей** информационной системы;
  - **порядок взаимодействия** с иными информационными системами (в случае предполагаемого взаимодействия), в том числе при осуществлении информационных отношений на правах операторов, посредников, пользователей информационных систем и обладателей информации.

ПОЛОЖЕНИЕ о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено

- **Пункт 10. Техническое задание** разрабатывается собственником (владельцем) информационной системы либо специализированной организацией и утверждается собственником (владельцем) информационной системы.
- **Техническое задание должно содержать:**
  - **наименование информационной системы** с указанием присвоенного ей класса типовых информационных систем;
  - **требования к системе защиты информации** в зависимости от используемых технологий и класса типовых информационных систем на основе перечня согласно приложению 3;
  - **сведения об организации** взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия) с учетом требований согласно приложению 4;
  - **требования к средствам криптографической защиты информации**, включая требования к криптографическим алгоритмам в зависимости от задач безопасности (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита), криптографическим протоколам, управлению криптографическими ключами (генерация, распределение, хранение, доступ, уничтожение), а также к функциональным возможностям безопасности и форматам данных. Профили требований, предъявляемых к средствам криптографической защиты информации, определяются Оперативно-аналитическим центром при Президенте Республики Беларусь (далее - ОАЦ);
  - **перечень документации на систему защиты информации**.
- Собственник (владелец) информационной системы вправе не включать в техническое задание отдельные обязательные требования к системе защиты информации при отсутствии в информационной системе соответствующего объекта (технологии) либо при условии согласования с ОАЦ закрепления в таком техническом задании обоснованных компенсирующих мер.

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
1	**Аудит безопасности**						
1.1	Определение состава информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности и другое)	+	+	+	+	+	+
1.2	Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	+	+	+	+	+	+
1.3	Обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	+/-	+/-	+/-	+/-	+/-	+

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
1.4	Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы	+	+	+	+	+	+
1.5	Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года	+	+	+	+	+	+
2	**Требования по обеспечению защиты данных**						
2.1	Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием	+	+	+	+	+	+

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
2.2	Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного про1раммного обеспечения и средств защиты информации	+	+	+	+	+	+
2.3	Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного про1раммного обеспечения, средств защиты информации и событиям безопасности	+	+	+	+	+	+
3	**Требования по обеспечению идентификации и аутентификации**						
3.1	Обеспечение разграничения доступа пользователей к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации	+	+	+	+	+	+

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
3.2	Обеспечение идентификации и аутентификации пользователей информационной системы	+	+	+	+	+	+
3.3	Обеспечение защиты обратной связи при вводе аутентификационной информации	+	+	+	+	+	+
3.4	Обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы	+	+	+	+	+	+
3.5	Обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы	+	+	+	+	+	+
3.6	Обеспечение централизованного управления учетными записями пользователей информационной системы и контроль за соблюдением правил генерации и смены паролей пользователей информационной системы	+/-	+/-	+/-	+/-	+	+

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
3.7	Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу	+	+	+	+	+	+
4	**Требования по защите системы защиты информации информационной системы**						
4.1	Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию	+	+	+	+	+	+
4.2	Обеспечение обновления объектов информационной системы	+	+	+	+	+	+
4.3	Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы	+	+	+	+	+	+

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
4.4	Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации	+	+	+	+	+	+
5	**Обеспечение криптографической защиты информации**						
5.1	Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного или предварительного шифрования)	+/-	+/-	+/-	+	+	+
5.2	Обеспечение конфиденциальности и контроля целостности информации при ее хранении в информационной системе (средства предварительного шифрования)	+/-	+/-	+/-	+/-	+/-	+/-

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
5.3	Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи)	+	+	+	+	+	+
5.4	Обеспечение контроля целостности данных в информационной системе (средства контроля целостности)	+/-	+/-	+/-	+/-	+/-	+/-
5.5	Обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены)	+/-	+/-	+	+/-	+/-	+
5.6	Обеспечение идентификации и аутентификации в информационной системе (криптографические токены)	+/-	+/-	+/-	+/-	+/-	+/-

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
6	**Дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре**						
6.1	Обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг	+/-	+/-	+	+	+	+
6.2	Обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин	+/-	+/-	+	+	+	+
6.3	Обеспечение безопасного перемещения виртуальных машин и обрабатываемых на них данных	+/-	+/-	+	+	+	+
6.4	Обеспечение резервного копирования пользовательских виртуальных машин	+/-	+/-	+	+	+	+
6.5	Обеспечение резервирования сетевого оборудования по схеме N+1	+/-	+/-	+/-	+	+	+

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
6.6	Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам	+/-	+	+	+/-	+	+
7	**Иные требования**						
7.1	Определение перечня разрешенного про1раммного обеспечения и регламентация порядка его установки и использования	+	+	+	+	+	+
7.2	Обеспечение контроля за составом объектов информационной системы	+	+	+	+	+	+
7.3	Автоматизированный контроль за составом средств вычислительной техники и сетевого оборудования	+/-	+/-	+/-	+/-	+	+

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
7.4	Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы)	+	+	+	+	+	+
7.5	Определение состава и содержания информации, подлежащей резервированию	+	+	+	+	+	+
7.6	Обеспечение резервирования информации, подлежащей резервированию	+	+	+	+	+	+
7.7	Обеспечение резервирования конфигурационных файлов сетевого оборудования	+/-	+/-	+/-	+	+	+
7.8	Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления	+	+	+	+	+	+

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
7.9	Обеспечение сегментирования (изоляции) сети управления объектами информационной системы от сети передачи данных	+/-	+/-	+/-	+/-	+	+
7.10	Обеспечение защиты средств вычислительной техники от вредоносных программ	+	+	+	+	+	+
7.11	Обеспечение в реальном масштабе времени автоматической проверки пакетов сетевого графика и файлов данных, передаваемых по сети, и обезвреживание обнаруженных вредоносных программ	+/-	+/-	+/-	+/-	+	+
7.12	Обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ	+/-	+/-	+/-	+	+	+

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
7.13	Обеспечение управления внешними информационными потоками (маршрутизация) между информационными системами. Использование маршрутизатора (коммутатора маршрутизирующего)	+/-	+/-	+/-	+	+	+
7.14	Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях	+/-	+/-	+/-	+	+	+/-
7.15	Обеспечение Ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, сетевом и прикладном уровнях	+/-	+/-	+/-	+/-	+/-	+

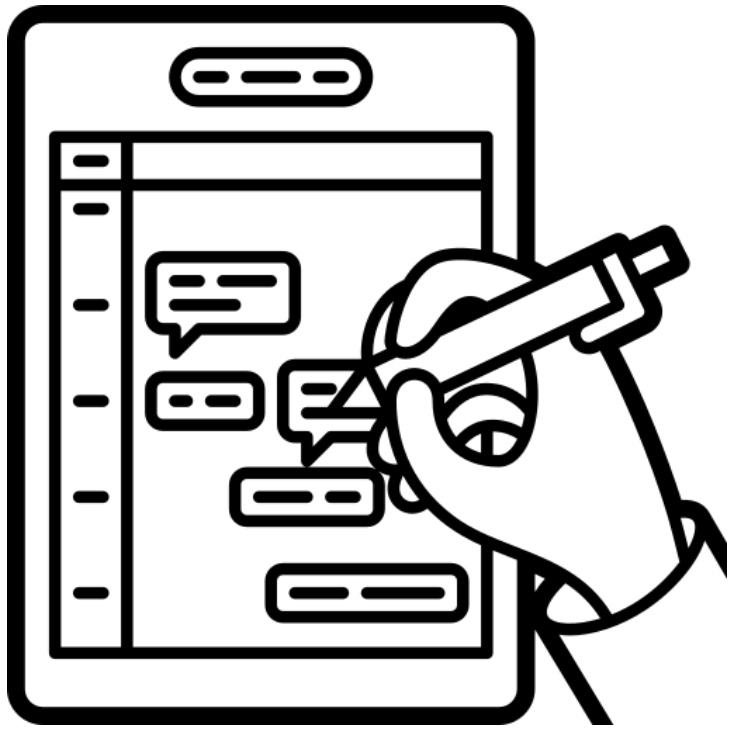
ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
7.16	Обеспечение обнаружения и предотвращения вторжений в информационной системе. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений	+/-	+/-	+/-	+	+	+
7.17	Обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и тому подобное). Использование беспроводных систем обнаружения и предотвращения вторжений	+/-	+/-	+/-	+	+	+
7.18	Обеспечение обнаружения и предотвращения утечек информации из информационной системы. Использование системы обнаружения и предотвращения утечек информации из информационной системы	+/-	+/-	+/-	+/-	+/-	+

ПЕРЕЧЕНЬ требований к системе защиты информации, подлежащих включению в техническое задание

№	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем					
		4-фл	4-юл	4-дсп	3-фл	3-юл	3-дсп
7.19	Определение перечня внешних подключений к информационной системе и порядка такого подключения	+/-	+/-	+/-	+	+	+
7.20	Обеспечение контроля за внешними подключениями к информационной системе	+/-	+/-	+/-	+	+	+
7.21	Ежегодное проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы	+/-	+/-	+/-	+/-	+/-	

1. Требования, отмеченные знаком «+», являются обязательными.
2. Требования, отмеченные знаком «+/–», являются рекомендуемыми.



5. Рекомендуемые области разработки политики информационной безопасности

5.2. The SANS Security Policy Project

The SANS Security Policy Project

Институт SANS США (www.sans.org) подготовил «**The SANS Security Policy Project**», который содержит большой репозитарий готовых ПБ на разные случаи жизни, распространяемых бесплатно. Также здесь можно найти интересные ссылки на ресурсы, посвященные разработке ПБ. Среди готовых ПБ Института SANS имеются политики, охватывающие следующие области разработки ПБ:

- допустимое шифрование,
- допустимое использование,
- аудит безопасности,
- оценка рисков,
- классификация данных,
- управление паролями,
- использование ноутбуков,
- построение демилитаризованной зоны,
- построение внутренней сети,
- безопасностей рабочих станций и серверов,
- антивирусная защита,
- безопасность маршрутизаторов и коммутаторов,
- безопасность беспроводного доступа,
- организация удалённого доступа,
- построение виртуальных частных сетей (VPN),
- безопасность периметра.

SANS Top 20 Critical Security Controls and Security Monitoring (SIEM)

Топ-20 самых важных защитных мер и средств

1. **Инвентаризация разрешенных и несанкционированно подключенных устройств.** Необходимо иметь полную информацию о подключенных к сети устройствах и блокировать несанкционированное подключение устройств.
2. **Инвентаризация разрешенного и несанкционированно установленного программного обеспечения.** Используйте специализированные программные средства для сбора информации об установленных на компьютерах сети приложениях и выявления неразрешенных программ.
3. **Безопасные настройки аппаратного и программного обеспечения** для серверов, рабочих станций и ноутбуков. Должны применяться безопасные настройки, а не настройки по умолчанию. Образы, с которых производится установка систем, должны быть предварительно настроены для обеспечения необходимого уровня защиты и протестированы. Должно быть организовано безопасное хранение этих образов.
4. **Безопасные настройки сетевых устройств** (межсетевых экранов, маршрутизаторов, коммутаторов и т.п.). Внедрите специализированные средства для оценки правильности работы устройств, осуществляющих фильтрацию трафика, которые выполняют поиск ошибок и несанкционированных изменений конфигураций.
5. **Защита периметра.** Создайте периметр сети с помощью межсетевых экранов, прокси, DMZ и систем IPS уровня сети. Проверьте обеспечиваемую ими защиту сканерами уязвимостей.

Топ-20 самых важных защитных мер и средств

6. **Сопровождение, мониторинг и анализ журналов регистрации событий.** Включите в системах, сетевых устройствах и межсетевых экранах функции журналирования событий. Анализируйте создаваемые журналы.
7. **Безопасность прикладного ПО.** Тестируйте разработанное и приобретенное ПО с помощью автоматизированных средств анализа или с посредством ручного тестирования на проникновение. Проводимые атаки должны приводить к автоматической генерации соответствующих предупреждений (алертов).
8. **Контроль использования административных привилегий.** Осуществляйте мониторинг использования и отслеживайте учетные записи, имеющие административные привилегии.
9. **Контроль доступа на основе принципа "должен знать".** Отделите критичные данные от менее критичных, контролируйте доступ к ним.
10. **Постоянный анализ уязвимостей и их устранение.** Внедрите эффективные средства для сканирования, которые, в частности, позволяют сравнивать полученные результаты с результатами предыдущего сканирования для определения произошедших изменений.
11. **Мониторинг и контроль учетных записей.** Настройте системы для записи детальной информации об использовании учетных записей, применяйте самостоятельно разработанные скрипты или специализированные приложения для анализа содержимого журналов регистрации событий.

Топ-20 самых важных защитных мер и средств

12. **Защита от вредоносного кода.** Используйте административные функции или корпоративные системы обеспечения безопасности конечных точек, чтобы проверить, что средства защиты от вредоносных программ и системы IPS/IDS уровня хоста функционируют на всех управляемых компьютерах сети.
13. **Ограничение и контроль сетевых портов, протоколов и служб.** Настройте системы так, чтобы минимизировать «атакуемую поверхность» (attack surface) - отключите неиспользуемые службы и протоколы, заблокируйте ненужные для работы порты, установите межсетевые экраны уровня хоста для повышения защиты.
14. **Защита и контроль беспроводных устройств.** При использовании беспроводных сетей, применяйте специализированные IDS. Проводите сканирование и мониторинг для обнаружения работающих беспроводных сетей.
15. **Предотвращение утечек данных.** Используйте решения DLP для выявления попыток вывода критичных данных за пределы сети компании, а также иной подозрительной активности в защищаемой сети.
16. **Обеспечение безопасности сети.** Применяйте лучшие практики в области безопасности при проектировании сети, настройке маршрутизаторов, коммутаторов, критичных серверов, межсетевых экранов, компонентов безопасности и групп клиентских компьютеров.

Топ-20 самых важных защитных мер и средств

17. **Тестирование на проникновение.** Подражайте действиям компьютерных злоумышленников при определении границ и подходов к проведению тестов на проникновение. Используйте сведения о выявленных недостатках для повышения безопасности.
18. **Организация реагирования на инциденты.** Разработайте детальные процедуры реагирования на инциденты. Периодически проводите обучение и практическую отработку этих процедур на основе сценариев.
19. **Организация возможностей восстановления данных.** Внедрите надежные и безопасные процедуры резервного копирования важных данных. Тестируйте восстановление различных систем с созданных копий на регулярной основе.
20. **Оценка навыков по безопасности, проведение необходимых тренингов.** Оценивайте знания и навыки сотрудников по вопросам безопасности, чтобы определить, достаточно ли их для выполнения сотрудниками своих ролей. При необходимости организуйте дополнительное обучение (повышение осведомленности).

SANS Top 20 Critical Security Controls (CIS Controls)

Топ-20 самых важных защитных мер и средств

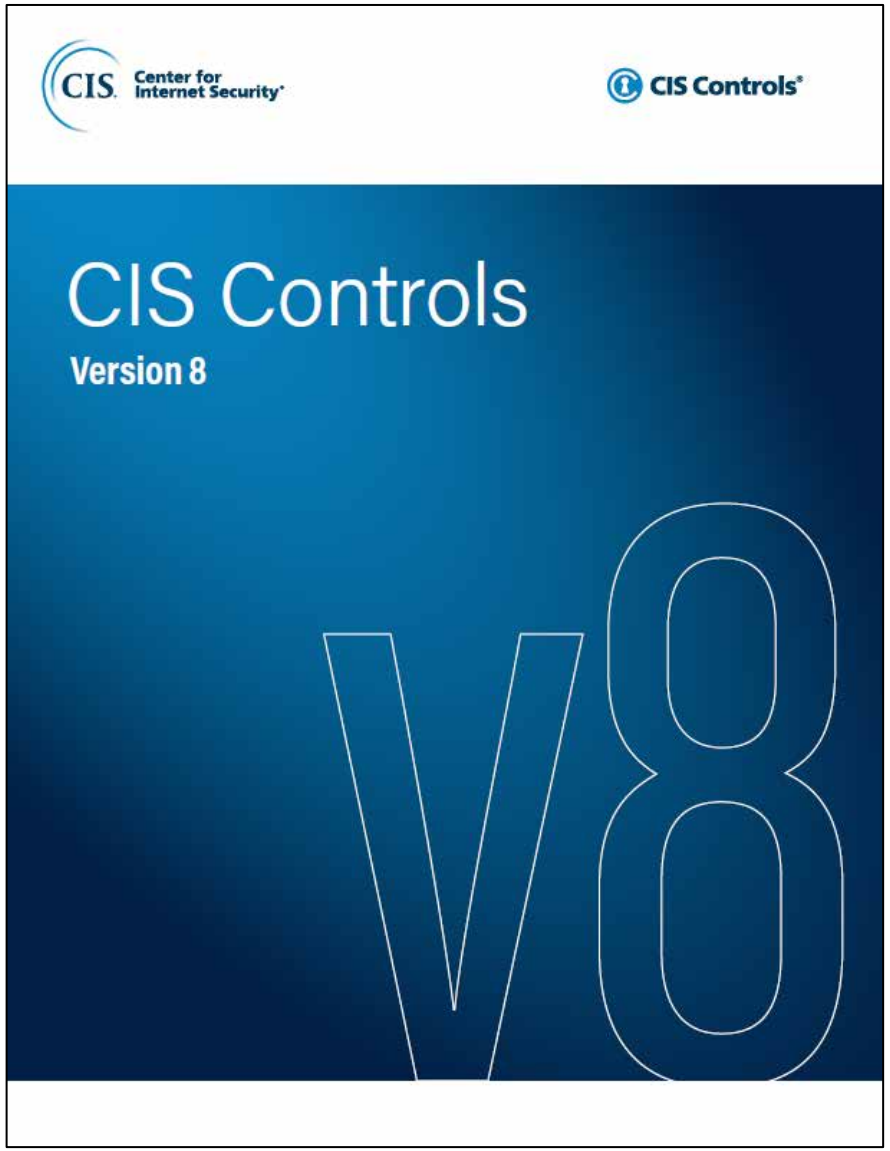
CIS Controls Version 7	
01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

CIS Controls Version 8	
01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

CIS Center for Internet Security®

CIS Controls v8. New v8 Released May 18, 2021
https://www.sans.org/blog/cis-controls-v8/

Руководство по кибербезопасности
CIS Controls Version 8



В CIS Controls Version 8
содержится 18 разделов, а внутри 153 практики.

CIS Controls Version 8

- 1. Инвентаризация и учет всех устройств
- 2. Инвентаризация и учет ПО
- 3. Защита данных
- 4. Защищенные конфигурации для устройств и ПО
- 5. Управление учетными записями
- 6. Управление контролем доступа
- 7. Непрерывное управление уязвимостями
- 8. Управление журналами аудита
- 9. Защита электронной почты и браузера
- 10. Защита от вредоносных программ

CIS Controls Version 8

- 11. Восстановление данных
- 12. Управление сетевой инфраструктурой
- 13. Сетевой мониторинг и защита
- 14. Осведомленность персонала и тренинги в области ИБ
- 15. Контроль безопасности сервис-провайдера (новое)
- 16. Управление безопасностью разработки прикладного ПО
- 17. Управление реакцией на инциденты ИБ
- 18. Тестирование на проникновение

С чего начать внедрение ИБ большим и маленьким: изучаем CIS Controls v8
https://habr.com/ru/company/dataline/blog/564414/

Защита информации

Тема: Политика информационной безопасности в организациях

Благодарю за внимание

КУТУЗОВ Виктор Владимирович

Список использованных источников

1. Рабочая программа дисциплины «Защита информации» / Кутузов В.В. – Могилев : Белорусско-Российский университет, 2019
2. Фотографии и картинки взяты с сайтов Яндекс.Картинки и Гугл.Картинки, иконки с flaticon.com
3. Основы информационной безопасности https://ppt-online.org/51922
4. Технические средства обеспечения безопасности: Учеб.-метод. пособие / Под ред. И. Е. Зуйкова.— Минск: БГПА. 2001 — 178 с https://rep.bntu.by/bitstream/handle/data/3612/Tekhnicheskie_sredstva_obespecheniya_bezopasnosti.pdf?sequence=1&isAllowed=y
5. Организационное поведение в бизнесе и управление сложными системами безопасности. Тема «Соотношение функций обеспечения безопасности, организационных и кадровых мер» https://electives.hse.ru/data/2017/02/03/1167518498/БПД4%202015%20тема%203.pdf
6. Системы оповещения людей о пожаре и управления эвакуацией https://do.ucp.by/pluginfile.php/15999/mod_folder/content/0/Лекции/Л.1.3.1%20Системы%20оповещения%20людей%20о%20пожаре%20и%20управления%20эвакуацией%20%28открытое%29.pdf?forcedownload=1
7. Системы контроля доступа https://ssbb.com.ua/sistemy-kontrolya-dostupa-skd
8. СОП предназначена для обнаружения нарушителя частной собственности и пресечения его дальнейшего проникновения на охраняемую территорию. https://tspplus.ru/security-systems/perimeter-security

Список использованных источников

9. Масштабная инсталляция системы распознавания лиц на 250 каналов реализована на VideoNet PSIM https://www.videonet.ru/krupnejshaya-sistema-raspoznavaniya-licz-na-250-kanalov-realizovana-na-videonet-psim.html
10. Пулко, Т. Л. Введение в информационную безопасность: учеб, пособие / Т. А. Пулко. - Минск : БГУИР, 2018. - 164 с. https://libeldoc.bsuir.by/bitstream/123456789/30130/3/Pulko_2018.pdf
11. Методические рекомендации по обеспечению информационной безопасности в Республике Беларусь. Система менеджмента информационной безопасности https://oac.gov.by/public/content/files/files/metod_recomend.docx
12. Практика ИБ \ SANS - Топ 20 наиболее критичных защитных мер и средств http://dorlov.blogspot.com/2011/06/sans-20.html
13. CIS Controls v8. New v8 Released May 18, 2021 https://www.sans.org/blog/cis-controls-v8/
14. CIS Controls https://www.cisecurity.org/controls/
15. Download the CIS Controls® v8 https://learn.cisecurity.org/cis-controls-download
16. Download the CIS Controls® V7.1 https://learn.cisecurity.org/CIS-Controls-v7.1
17. С чего начать внедрение ИБ большим и маленьким: изучаем CIS Controls v8 https://habr.com/ru/company/dataline/blog/564414/

Список использованных источников

18. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 20.02.2020 № 66 «ПОЛОЖЕНИЕ о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено» https://pravo.by/upload/docs/op/T62004470_1582923600.pdf