АССОЦИАЦИЯ
ЛИГА СОДЕЙСТВИЯ
ОБОРОННЫМ
ПРЕДПРИЯТИЯМ

Формирование единой Политики информационной безопасности для предприятий оборонно-промышленного комплекса Российской Федерации

г. Москва 2021 г.

Основные рассматриваемые вопросы:

1. Современные реалии и вызовы для промышленных предприятий ОПК
2. Угрозы безопасности информации
3. Политика ИБ - руководящие и рекомендательные документы
4. Разработка и внедрение Политики ИБ
5. Пример Политики ИБ

Основная функция ОПК – создание, поставка и поддержание эксплуатации образцов вооружений и военной и специальной техники, приобретаемой как вооруженными силами в рамках их технического оснащения, так и другими странами – в рамках военно-технического сотрудничества.

Но ОПК также выполняет и роль научно-технической и технологической базы по ряду направлений инновационного развития экономики страны.

Современные реалии и вызовы для промышленных предприятий ОПК

• Совершенствование бизнес-процессов

Бизнес-процесс – это совокупность взаимосвязанных мероприятий или задач, которые имеют определенные временные рамки, конкретные ресурсы на входе, и направлены на создание определённого продукта или услуги для потребителей.

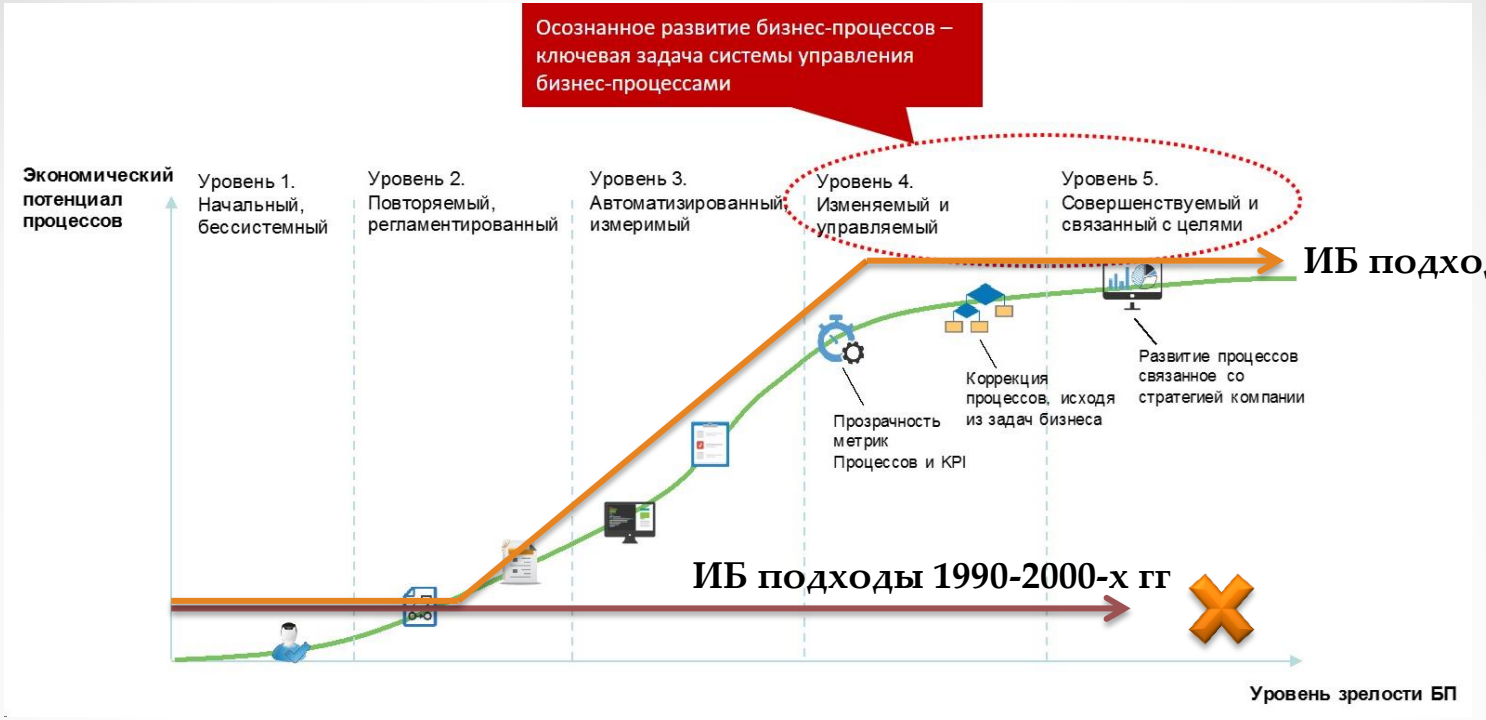
Под влиянием изменчивых требований конкурентной среды менеджмент процессов постоянно дополняется и изменяется.

Оптимизация бизнес-процессов – это частичное улучшение, которое происходит путем избавления от явных недостатков, таких как информационные петли, дублирование функций и т.п., а также увязывание различных бизнес-действий между собой.

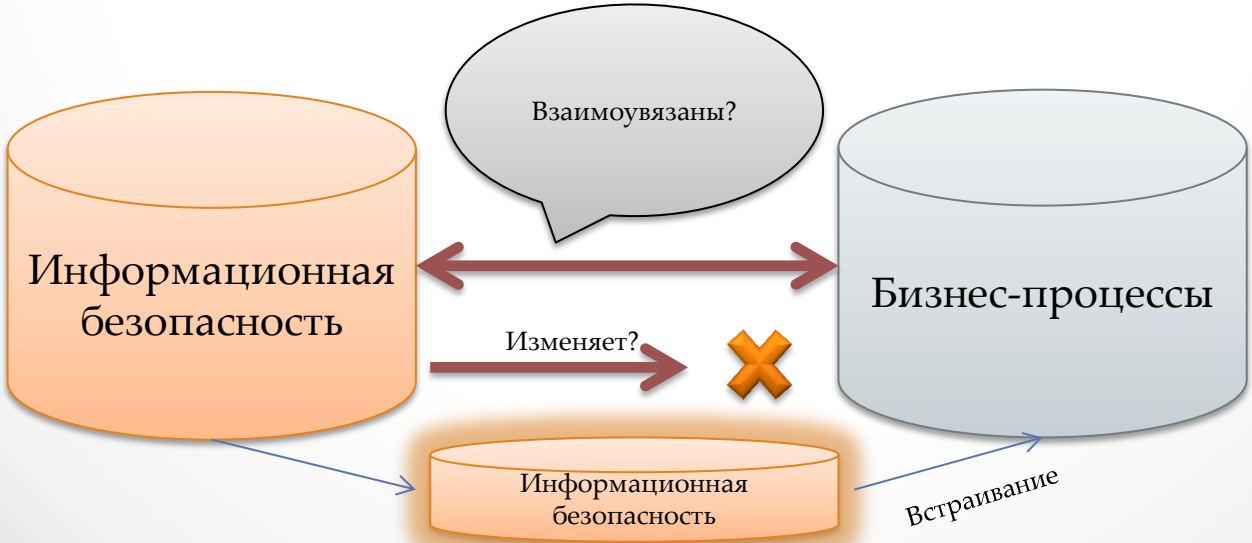
Совершенствование (улучшение) бизнес-процессов – это непрерывный процесс анализа действующих процессов, поиск и устранение как видимых, так и скрытых проблем, с целью повышения эффективности деятельности предприятия.

Источник: http://sisupr.mrsu.ru/2016-2/PDF/Efremova.pdf

https://www.elmabpm.ru/journal/postroenie-sistemy-upravleniya-biznes-processami-v-krupnoj-kompanii/



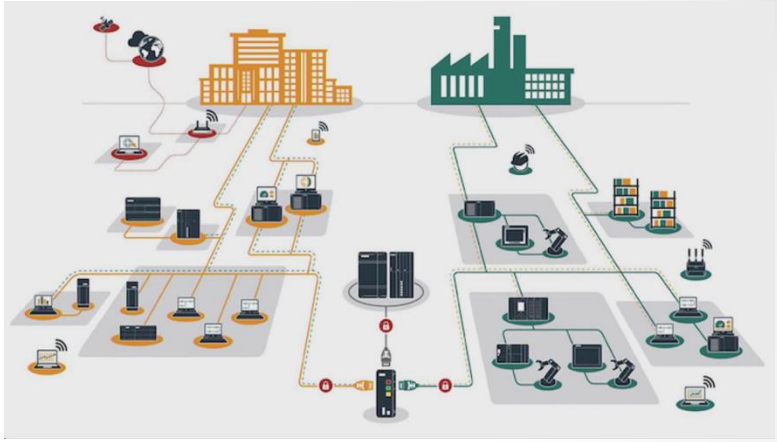
Основная задача системы управления бизнес-процессами – развитие процессов, которое позволяет увеличить экономический потенциал с операционной и стратегической точек зрения.



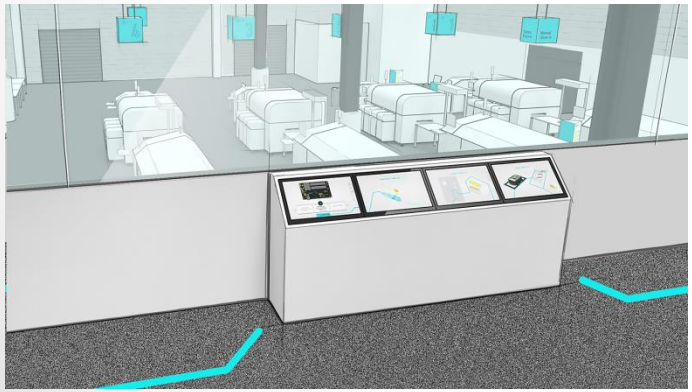
- **Автоматизация производства**

- АСУ ТП;
- Станки с числовым программным управлением;
- Цифровые копии
- Увеличение числа АРМ и АС

- **Внедрение на предприятиях ОПК технологий цифрового производства**



Пример цифрового завода

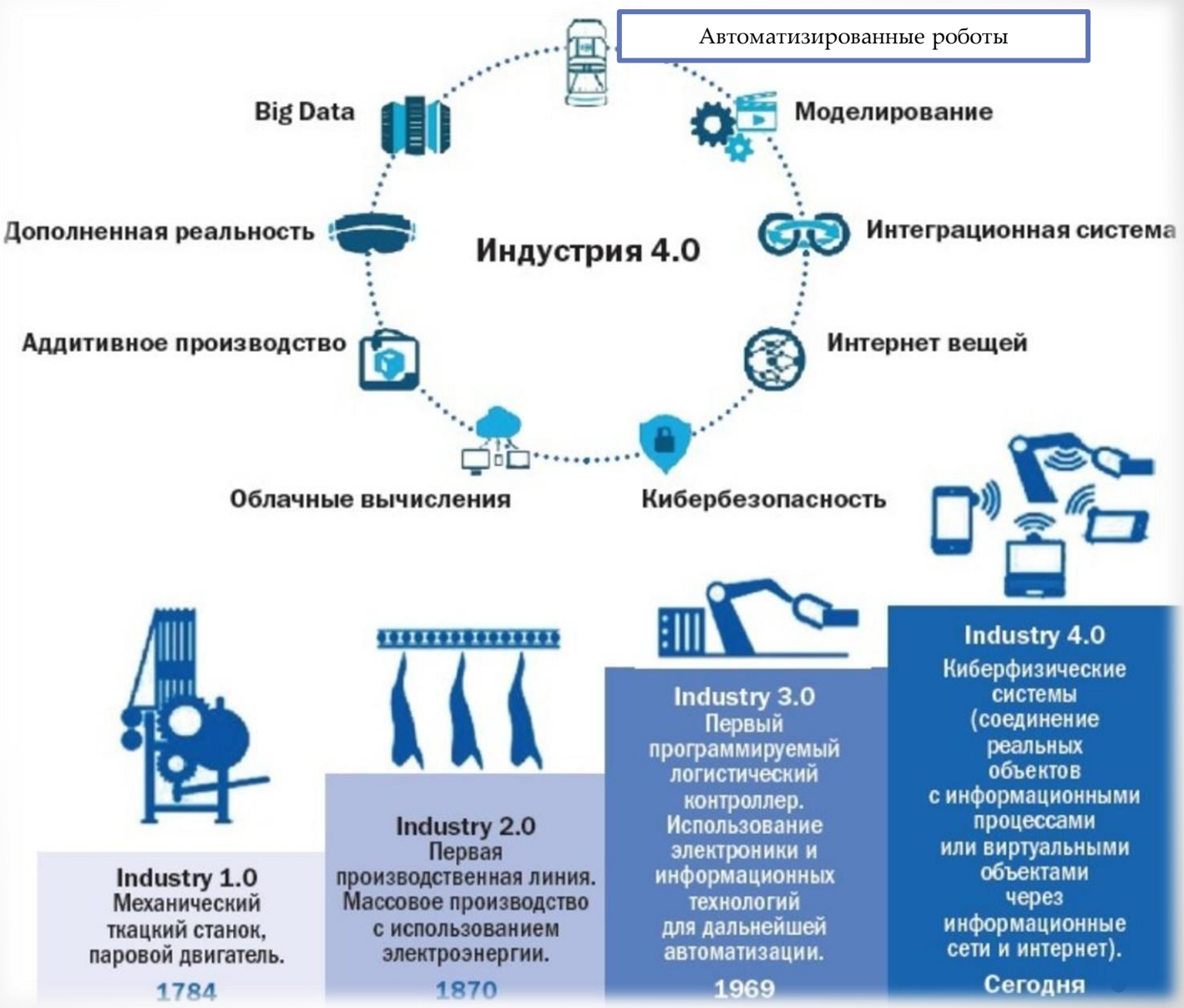


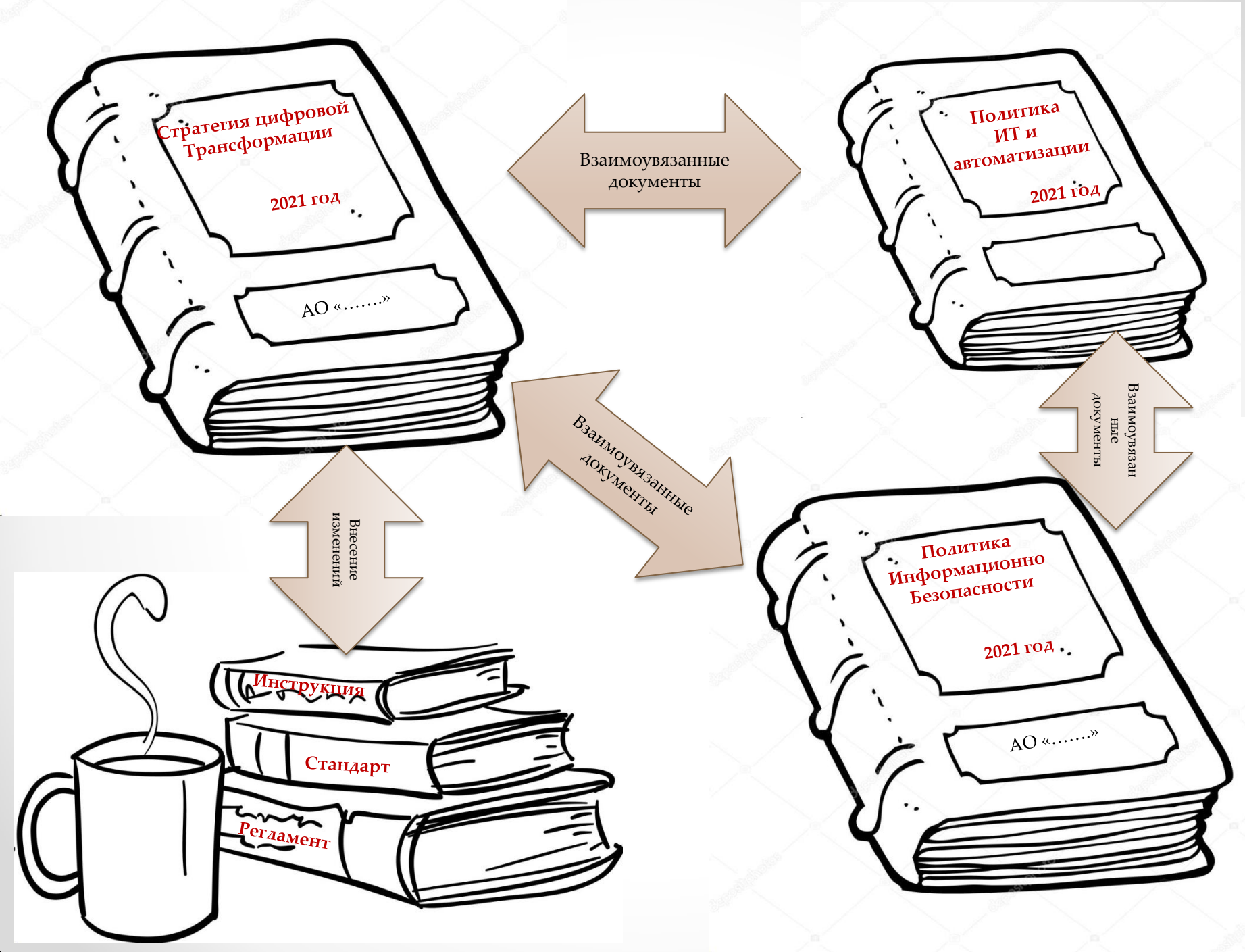
Задачами цифровизации производства являются задачи создания и внедрения на предприятии современных интегрированных информационных систем и передовых производственных технологий, цифровых фабрик, охватывающих все бизнес-процессы и подразделения предприятия, а также все стадии ЖЦ производимых изделий.

- **Внедрение технологий 4-й Промышленной революции**

В характеристику Четвертой промышленной революции входят следующие инновации:

- Интернет вещей.
- Облачные технологии и цифровые платформы.
- 3D принтеры, моделирование.
- Синтез пищи.
- Автоматизированные роботы, самоуправляемые машины.
- Нейросети.
- Генная модификация.
- Биотехнологии.
- Искусственный интеллект (ограниченный, общий, суперинтеллект).




Стратегия цифровой Трансформации
2021 год
АО «……»
Взаимоувязанные документы
Политика ИТ и автоматизации
2021 год
Взаимоувязанные документы
Взаимоувязанные документы
Внесение изменений
Политика Информационно Безопасности
2021 год
АО «……»
Инструкция
Стандарт
Регламент

- **Диверсификация производства**

Диверсификация производства

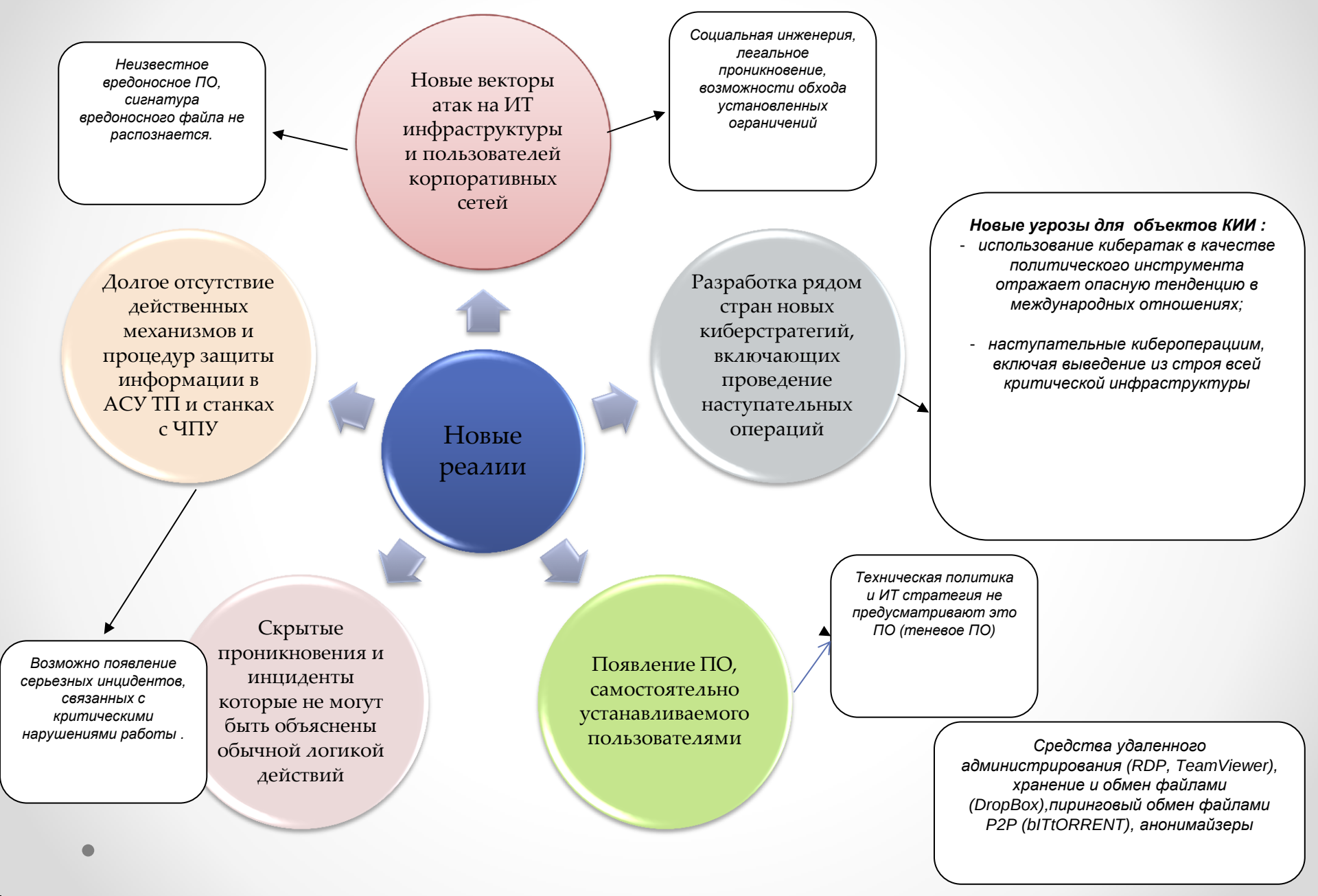
расширение ассортимента, изменение вида продукции, производимой предприятием, фирмой, освоение новых видов производств с целью получения экономической выгоды

Мы переходим к новой индустриальной модели, и диверсификация предприятий ОПК в этом смысле, по сути, **знаменует этот переход**.

Диверсификация – это расширение линейки продукции, это захват новых рынков, это выпуск высокотехнологичных востребованных товаров.

Угрозы информационной безопасности

Новые угрозы



Новые вызовы ИБ – **сотрудник** предприятия

Конфиденциальная информация

На работе

Система защиты информации строится отделом ИБ

Правила и ограничения

?

Личная почта

Личная почта

Социальные сети: анализ предпочтений, запросов, и пр.

Искусственный интеллект: анализ предпочтений, запросов, и пр.

Функциональные обязанности

?

?

?

Информационные потоки

Дома

Система защиты информации строится самостоятельно

В отпуске

?

Социальные сети: анализ предпочтений, запросов, и пр.

Искусственный интеллект: анализ предпочтений, запросов, и пр.

Интернет провайдер

Искусственный интеллект: анализ предпочтений, запросов, и пр.

Социальные сети: анализ предпочтений, запросов, и пр.

?

Интернет провайдеры

Количество и анализ всех подключенных устройств

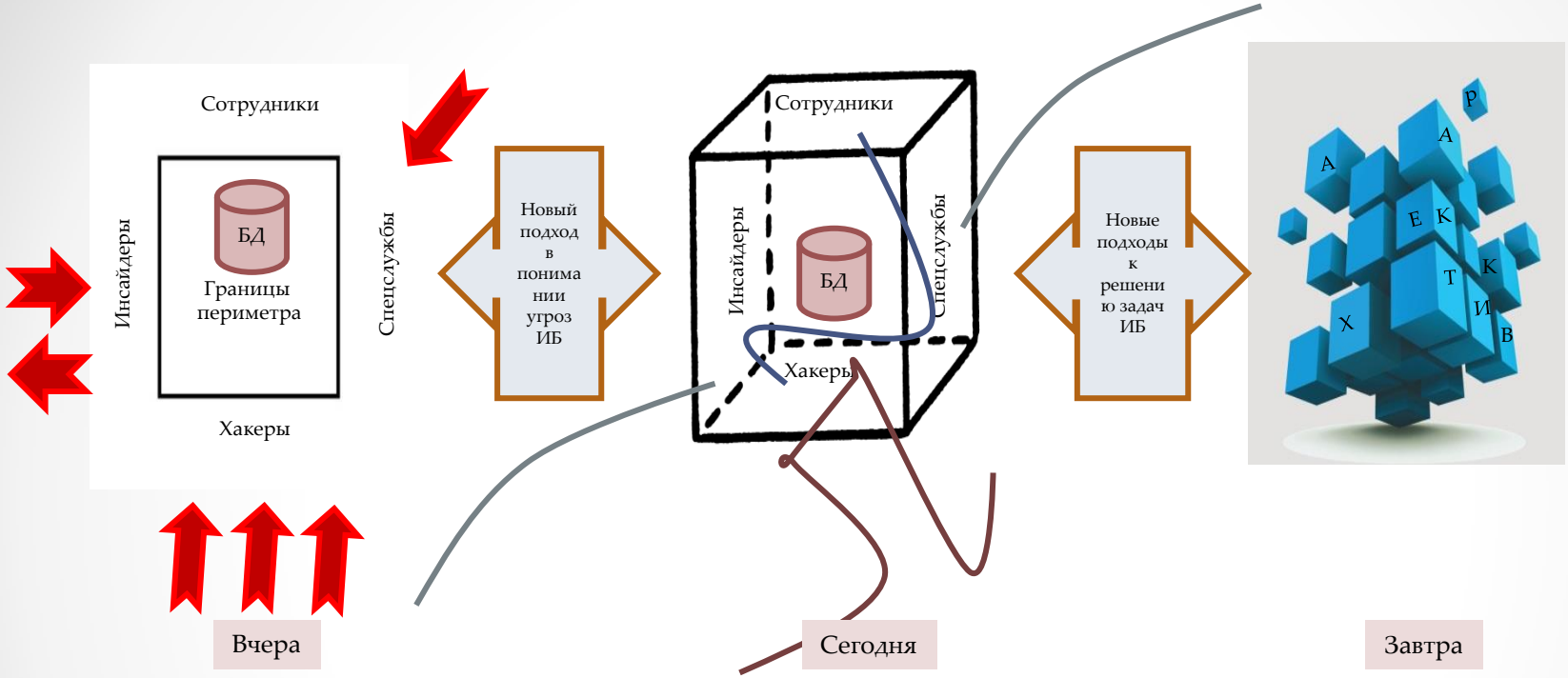
Количество и анализ всех подключенных устройств

?

Дополнительная работа, майнинг

Современное понимание ИБ

Новое видение подходов к обеспечению ИБ

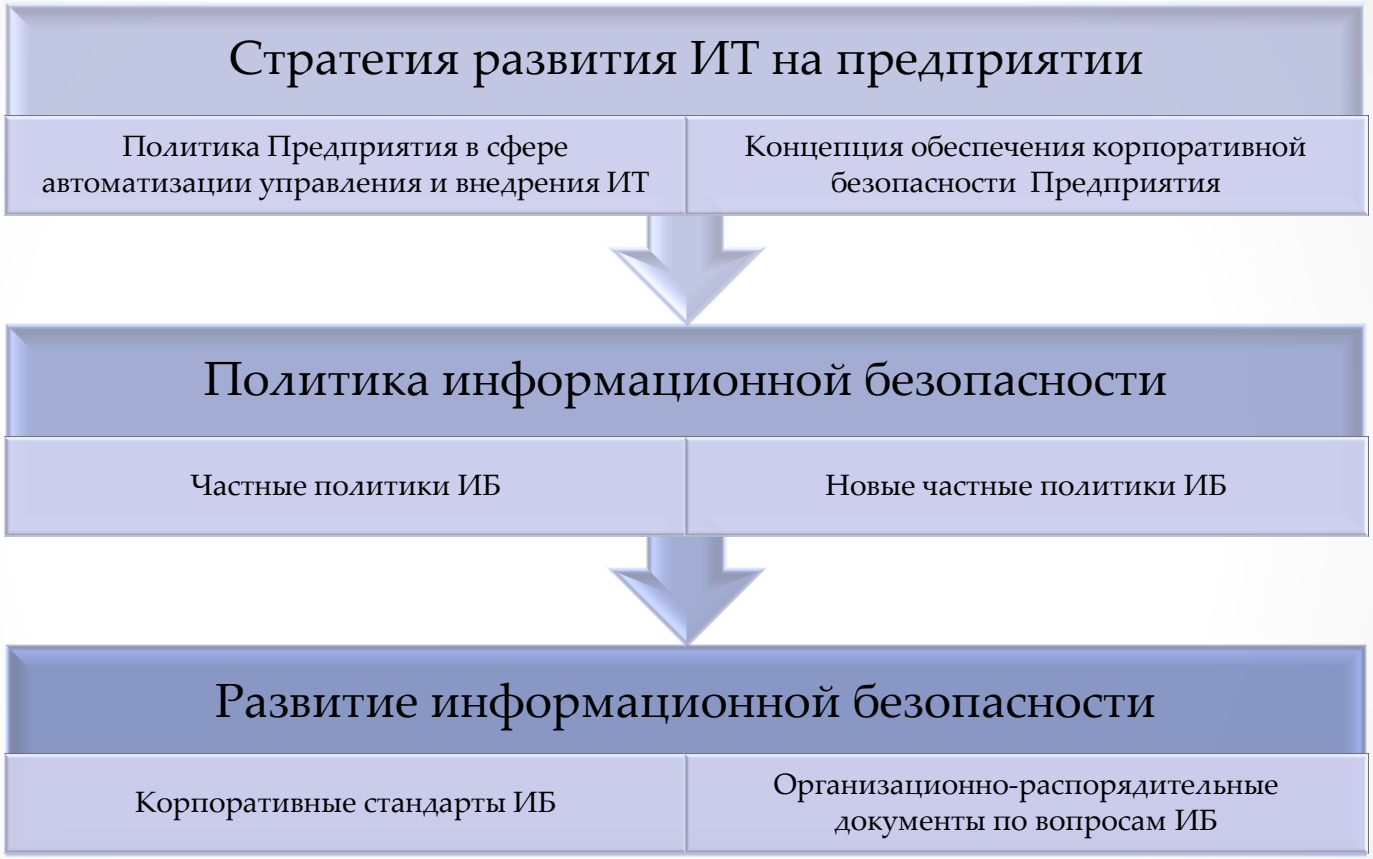


Ландшафт угроз уже изменился…

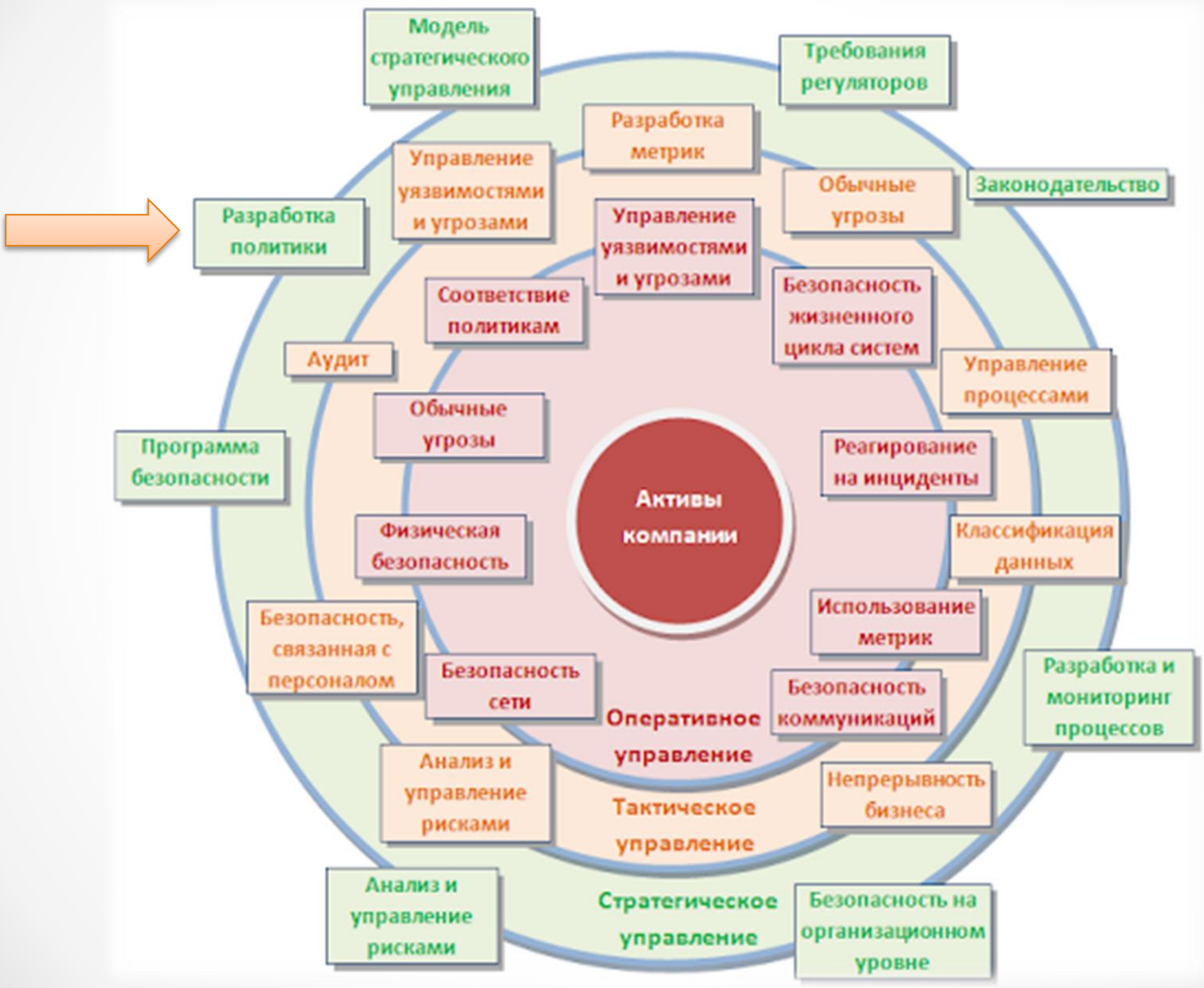
Основная задача: Сохранить активы, исключить возможность работы злоумышленника и нанесение им вреда в том числе и при попытках использования вредоносного ПО.

«Ландшафт угроз сегодня невероятно сложен, динамичен и целенаправлен – требуется иной уровень интеллекта, чтобы понимать и управлять им»
Источник: из презентации SIEM решения IBM

Стратегия развития ИТ и ИБ на предприятии



Пример: Политика ИБ в управлении безопасностью информации



Источник: схема взята из сети Интернет

Политика ИБ предприятия учитывает

Область применения Политики ИБ

Политика информационной безопасности является методологической основой для:

Формирования единой информационно-правовой базы в области обеспечения информационной безопасности	Принятия управленческих решений и разработке практических мер, направленных на предотвращение угроз безопасности информации, уменьшение вероятности реализации или снижение ущерба при реализации	Координации деятельности структурных подразделений по вопросам информационной безопасности

Проект Политики ИБ разрабатывается с учетом действующих Национальных стандартов РФ (требований ГОСТ Р ИСО/МЭК 27002 и ГОСТ Р ИСО/МЭК 27003, введены в действие в 2013 - 2014 годах), а также основных понятийных требований к разрабатываемым высоко уровневым документам по ИБ.

ГОСТ Р ИСО/МЭК 27002-2012 Группа Т00

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Свод норм и правил менеджмента информационной безопасности

Information technology. Security techniques. Code of practice for information security management

ГОСТ Р ИСО/МЭК 27003-2012

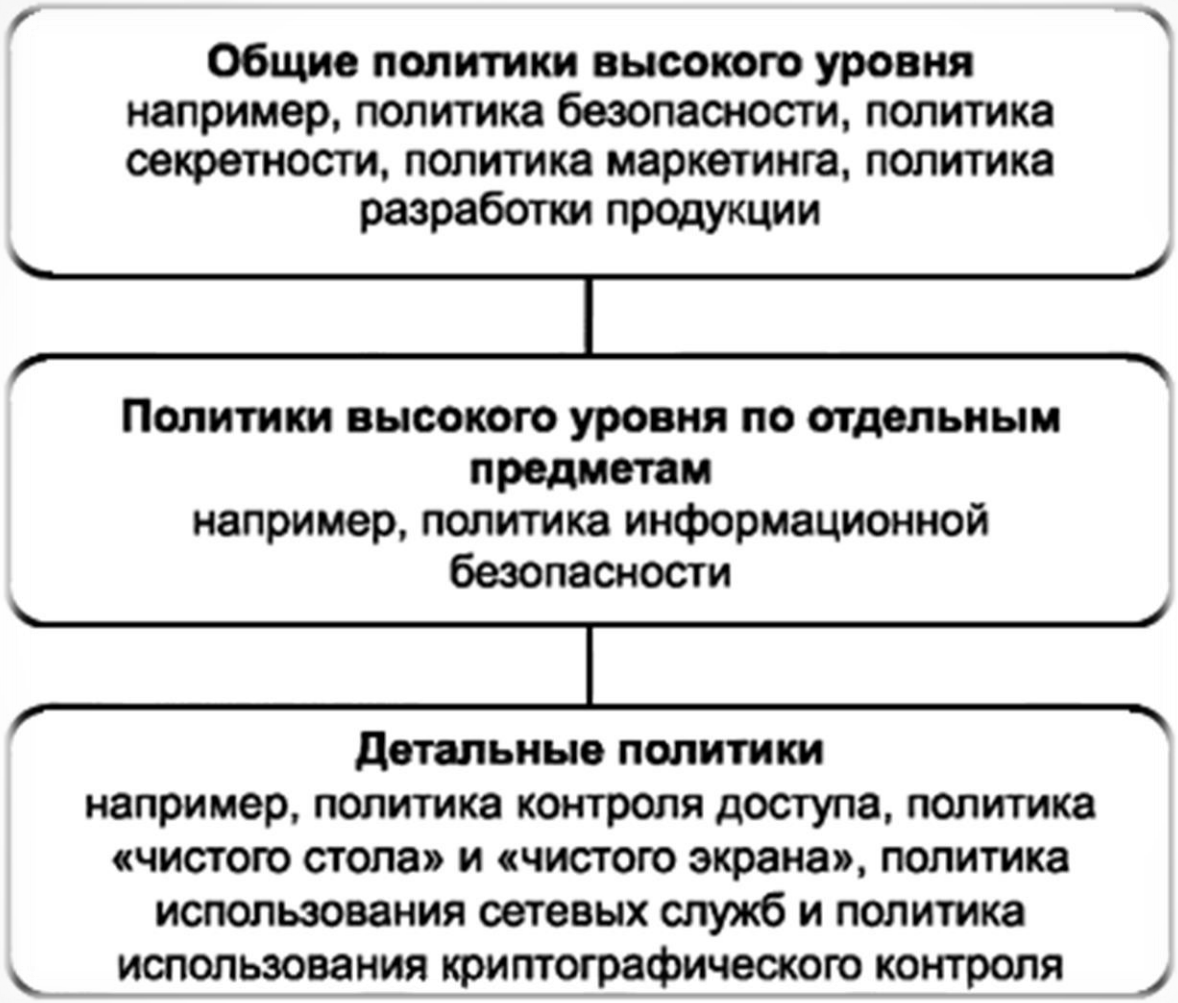
НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности

Information technology. Security techniques. Information security management systems implementation guidance

Иерархия политики по ГОСТ Р ИСО/МЭК 27003-2012



Политика информационной безопасности
(по ГОСТ Р ИСО/МЭК 27002)

Цель: ***Обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с требованиями бизнеса и соответствующими законами и нормами.***

- ***Высшее руководство должно установить четкое направление политики в соответствии с целями бизнеса и демонстрировать поддержку и обязательства в отношении обеспечения информационной безопасности посредством разработки и поддержки политики информационной безопасности в рамках организации.***
- При необходимости следует предусмотреть наличие контактного лица, занимающегося вопросами информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники.
- Следует налаживать контакты с внешними специалистами по безопасности или группами специалистов, включая соответствующие органы, чтобы находиться в курсе отраслевых тенденций, осуществлять мониторинг стандартов и методов оценки, и обеспечивать адекватные точки контакта при обработке инцидентов информационной безопасности.
- Следует поощрять многопрофильный подход к обеспечению информационной безопасности.

Целью создания Политики ИБ является определение стратегии Предприятия ОПК в области ИБ. Основными целями предприятия в области обеспечения ИБ являются:

1. Эффективная защита информационных активов предприятия

2. Защита предприятия от возможного нанесения материального, репутационного, морального или иного вида ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи.

3. Соответствие требованиям законодательных и нормативных документов

Указанные цели достигаются посредством обеспечения и постоянного поддержания следующих основных свойств информации:

- **доступности** информации для легальных пользователей (устойчивого функционирования автоматизированных систем и компонентов информационной инфраструктуры, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);

- **целостности и аутентичности** (подтверждение авторства) информации, хранимой, обрабатываемой и передаваемой по каналам связи;

- **конфиденциальности** - сохранения в тайне информации, хранимой, обрабатываемой и передаваемой по каналам связи.

Разработка политики информационной безопасности

Политика информационной безопасности документирует стратегическую позицию организации в отношении информационной безопасности во всей организации.

- Политика строится на основе информации и знания. Моменты, признанные руководством важными во время ранее проведенного анализа, должны быть сделаны наглядными, им должно быть уделено особое внимание в политике, чтобы обеспечить стимуляцию и мотивацию в организации. Также важно отметить, что происходит, если не следовать выбранной политике, и подчеркнуть влияния законов и регулирующих положений на рассматриваемую организацию.

- Примеры политики информационной безопасности можно взять из справочной литературы, сети Интернет, в сообществах по интересам и отраслевых объединениях. Формулировки и подсказки можно найти в годовых отчетах, других документах по политике или документах, сохраняемых руководством.

- Относительно фактического объема документации по политике могут существовать различные интерпретации и требования. Эта документация должна быть в достаточной степени суммирована, чтобы работники организации понимали значение политики. Кроме того, она должна достаточно четко показывать, каких целей необходимо достичь, чтобы установить набор правил и целей организации.

- Объем и структуру политики информационной безопасности должны подкреплять документы, которые используются на следующем этапе процесса, для введения системы управления информационной безопасностью.

- Для больших организаций со сложной структурой (например, с широким спектром различных областей деятельности) может возникнуть необходимость создания общей политики и множества политик более низкого уровня, адаптированных к конкретным областям деятельности.

Предлагаемая политика (с номером версии и датой) должна быть подвергнута перекрестной проверке и учреждена в организации оперативным руководителем. После учреждения в группе управления или аналогичном органе оперативный руководитель утверждает политику информационной безопасности.

Затем она доводится до сведения каждого работника организации надлежащим способом, чтобы стать доступной и понятной для читателей.

Правильное понимание целей и задач

Политика ИБ необходима для того, чтобы донести до руководства и сотрудников цели и задачи информационной безопасности компании. Бизнес руководство и сотрудники должны понимать, что сотрудник ИБ это не только инструмент для расследования фактов утечек данных, но и помощник в минимизации рисков компании, а следовательно — в повышении прибыльности и успешности предприятия (организации).

Политика ИБ необходима главным образом и для обоснования введения защитных мер в компании.

Политика соответственно должна быть утверждена высшим административным органом компании (генеральный директор, совет директоров и т.п.).

Любая рассматриваемая к применению защитная мера всегда является компромиссом между снижением рисков и удобством работы для обычного пользователя корпоративной сети предприятия.

Когда сотрудник ИБ говорит, что рабочий процесс не должен происходить каким-либо образом по причине появления некоторых рисков, ему всегда задают резонный вопрос:

«А как тогда он должен происходить?»

И в этом случае сотруднику ИБ необходимо предложить такую модель процесса, в которой эти риски будут снижены в какой-то допустимой мере, удовлетворительной и полностью приемлемой для обеспечения рабочих повседневных процессов предприятия.

Политика ИБ может иметь следующую структуру:

1. **Краткое изложение политики** - общее описание из одного-двух предложений. (Иногда может объединяться с введением).

2. **Введение** - краткое объяснение предмета политики.

3. **Область действия** - описывает части или действия организации, находящиеся под влиянием политики. При необходимости в пункте "Область действия" перечисляются другие политики, подкрепляемые данной политикой.

4. **Цели** - описание назначения политики.

5. **Принципы** - описание правил, касающихся действий и решений для достижения целей. В некоторых случаях может быть полезным определить ключевые процессы, связанные с предметом политики, и затем - правила выполнения процессов.

6. **Сферы ответственности** - кто отвечает за действия по выполнению требований политики. В некоторых случаях этот пункт может содержать описание организационных соглашений, а также сферы ответственности лиц с определенными ролями.

7. **Ключевые результаты** - описание результатов, получаемых предприятием, если цели достигнуты.

8. **Связанные политики** - описание других политик, относящихся к достижению целей, обычно с представлением дополнительных подробностей, касающихся отдельных предметов.

Документирование политики информационной безопасности

Политика информационной безопасности должна быть утверждена руководством, издана и доведена до сведения всех сотрудников организации и соответствующих сторонних организаций.

Политика информационной безопасности должна пересматриваться либо через запланированные интервалы времени, либо, если произошли значительные изменения, с целью обеспечения уверенности в ее актуальности, адекватности и эффективности.

Рекомендация по реализации

Политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к менеджменту информационной безопасности.

Документ, в котором излагается политика, должен содержать положения относительно:

a) определения информационной безопасности, ее общих целей и сферы действия, а также упоминания значения безопасности как инструмента, обеспечивающего возможность совместного использования информации;

b) изложения намерений руководства, поддерживающих цели и принципы информационной безопасности в соответствии со стратегией и целями бизнеса;

c) подхода к установлению мер и средств контроля и управления и целей их применения, включая структуру оценки риска и менеджмента риска;

d) краткого разъяснения наиболее существенных для организации политик безопасности, принципов, стандартов и требований соответствия.

Ключевые результаты Политики ИБ

Частные политики ИБ

Для реализации требований Политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности предприятия, разрабатываются частные политики по обеспечению ИБ. Данные документы оформляются как отдельные внутренние нормативные документы, согласовываются и утверждаются в соответствии с установленным порядком.

Перечень возможных частных политик ИБ:

- Политика контроля защищенности информационных активов;
- Политика обеспечения информационной безопасности при разработке, внедрении и эксплуатации автоматизированных систем;
- Политика парольной защиты;
- Политика антивирусной защиты;
- Политика безопасности АСУ ТП и станков с числовым программным управлением;
- Политика безопасности при использовании технологий виртуализации и облачных вычислений;
- Политика использования съемных носителей информации;
- Политика безопасности при использовании ресурсов сети «Интернет», удаленного доступа и мобильных технологий;
- Политика повышения осведомленности работников в области ИБ;
- Политика разграничения прав доступа;
- Политика криптографической защиты информации;
- Политика копирования и уничтожения информации;
- Политика мониторинга и аудитов ИБ;
- Политика кибербезопасности;
- Политика организации управления ИБ;
- Политика информационного противодействия в конкурентной среде;
- Политика управления затратами на обеспечение ИБ;
- Политика разработки и внедрения перспективных систем ИБ в образцах выпускаемых изделий;
- Политика организации обработки и обеспечения безопасности персональных данных.

Пример: необходимость внедрения политик второго уровня

Конфиденциальная информация в АС не защищена и не контролируется

Конфиденциальная информация в АС защищена и контролируется

Спасибо за внимание!

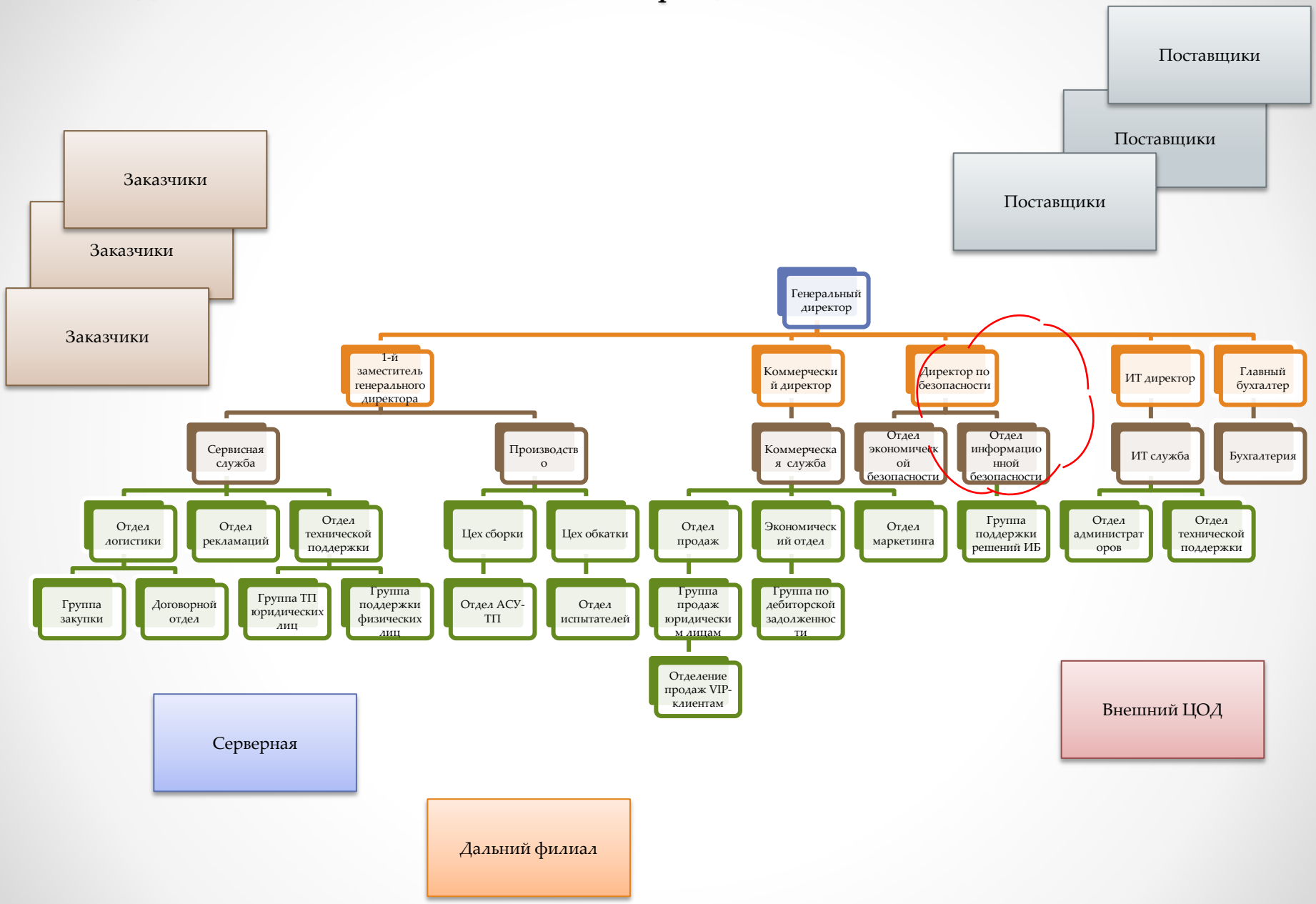
Олег Кузьмин
E-mail: olegnk2@yandex.ru

В заключении, несколько слов об организации работ и самообразовании специалистов ИБ

Психология информационной безопасности - молодое, но быстро развивающееся направление психологической науки. Это совершенно новое научное направление, которое призвано интегрировать подходы психологии как науки и информационной безопасности как направления (процесса) деятельности в исследовании поведения субъекта. Сочетание этих двух подходов позволяет более полно изучить поведение человека в ситуациях, связанных с практическим применением мерам информационной безопасности.

В нашем случае под психологией ИБ следует понимать - возможность и границы применимости человеком информационной безопасности как процесса на всех имеющихся технологических и социальных уровнях ее проявления в организации или на предприятии

Где начинается и заканчивается процесс обеспечения ИБ ?



Что должен знать современный специалист ИБ?

Системное мышление – это тип мышления, который характеризуется целостным восприятием предметов и явлений, учитывая их связи между собой. Каждый материальный объект, предмет, явление, процесс, научная теория, художественный образ и прочее представляет собой определенную систему.

Информационная безопасность нового типа

Системный анализ — научный метод познания, представляющий собой последовательность действий по установлению структурных связей между переменными или постоянными элементами исследуемой системы.