ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Институт техники и цифровых технологий
Факультет инфокоммуникационных систем и технологий
Кафедра информационной безопасности
Дисциплина: «Комплексное обеспечение ЗИ объекта информатизации (предприятия)»

Тема:
Обоснование требований к системе защите значимого объекта критической информационной инфраструктуры

Выполнила студентка группы ИБО-16/1:

Половинкина Вероника Валерьевна

Проверил: к.т.н. Журавлев С.И

Королев, 2019

Введение

Цель курсового проекта обоснование требований к системе защите значимого объекта критической информационной инфраструктуры и совершенствование программно-аппаратной защиты.

Для достижения поставленной цели необходимо решение следующих **задач:**

1. Анализ процесса формирования требований к системам безопасности объектов критических информационных инфраструктур;
2. Категорирование объектов КИИ, требования к системам безопасности и обеспечению безопасности значимых объектов КИИ;
3. Обеспечения безопасности объектов критических важных информационных инфраструктур с помощью АСУ ТП.

Объектом исследования в данной работе является КИИ, в частности, его подсистема программно-аппаратной защиты.

Предметом исследования следует рассматривать существующие технологии обеспечения информационной безопасности КИИ.

Анализ процесса формирования требований к системам безопасности объектов КИИ

(начало)

При определении требований СБО вновь создаваемые КИИ необходимо учитывать следующее:

1. Современный этап развития характеризуется переходом от экстенсивных к интенсивным путям повышения эффективности за счет качественного совершенствования КИИ и их СБО.

2. Сложность, высокая стоимость и новизна перспективных КИИ требуют системного, комплексного подхода к решению вопросов их создания и эксплуатации на основе широкого использования современных методов управления, обеспечивающих создании КИИ с внедренными СБО с заданными технико-экономическими и эксплуатационными характеристиками при минимальных затратах.

3. Разработка СБО перспективных КИИ должна обеспечивать следующих общих целей:

- достижение конечных целей эксплуатации КИИ при минимальных затратах совокупного ряда;
- минимизация численности потребного личного состава;
- снижение занятости личного состава;
- сокращение общей продолжительности работ, проводимых на КИИ;
- уменьшение продолжительности понижения готовности КИИ;
- уменьшение времени восстановления готовности КИИ при проведении работ на них;
- безопасность при проведении работ на КИИ;
- защищенность КИИ от НСД;
- повышение эффективности СБО, необходимого ресурса и срока службы КИИ и т.п.

Анализ процесса формирования требований к системам безопасности объектов КИИ

(окончание)

4. Процессу формирования требований к СБО КИИ должен предшествовать этап разработки сценария, т.е. качественное описание структуры создаваемого КИИ, возможных условий её эксплуатации, целей и задач СБО, принципов формирования и реализации целевых нормативов.

5. Проведение исследований по обеспечению формирования требований к СБО КИИ должно включать:

- Формулировку целей (постановку задачи) и неформальное задание критерия оптимальности;
- Построение математической модели принятия решений (определение математического выражения для критерия оптимальности «целевой функции» и ограничений), сбор данных и нормативов для решения задачи;
- Определение алгоритма поиска оптимального решения;
- Проверку модели и оценку решения;
- Реализацию (осуществления) решения.

6. Практические возможности применения математических моделей и методов формирования требований к СБО вновь создаваемых КИИ ограничиваются, в первую очередь, наличием факторов неопределенности исходной ин-формации о развитии научно-технического прогресса, поведения внешней среды, и др.

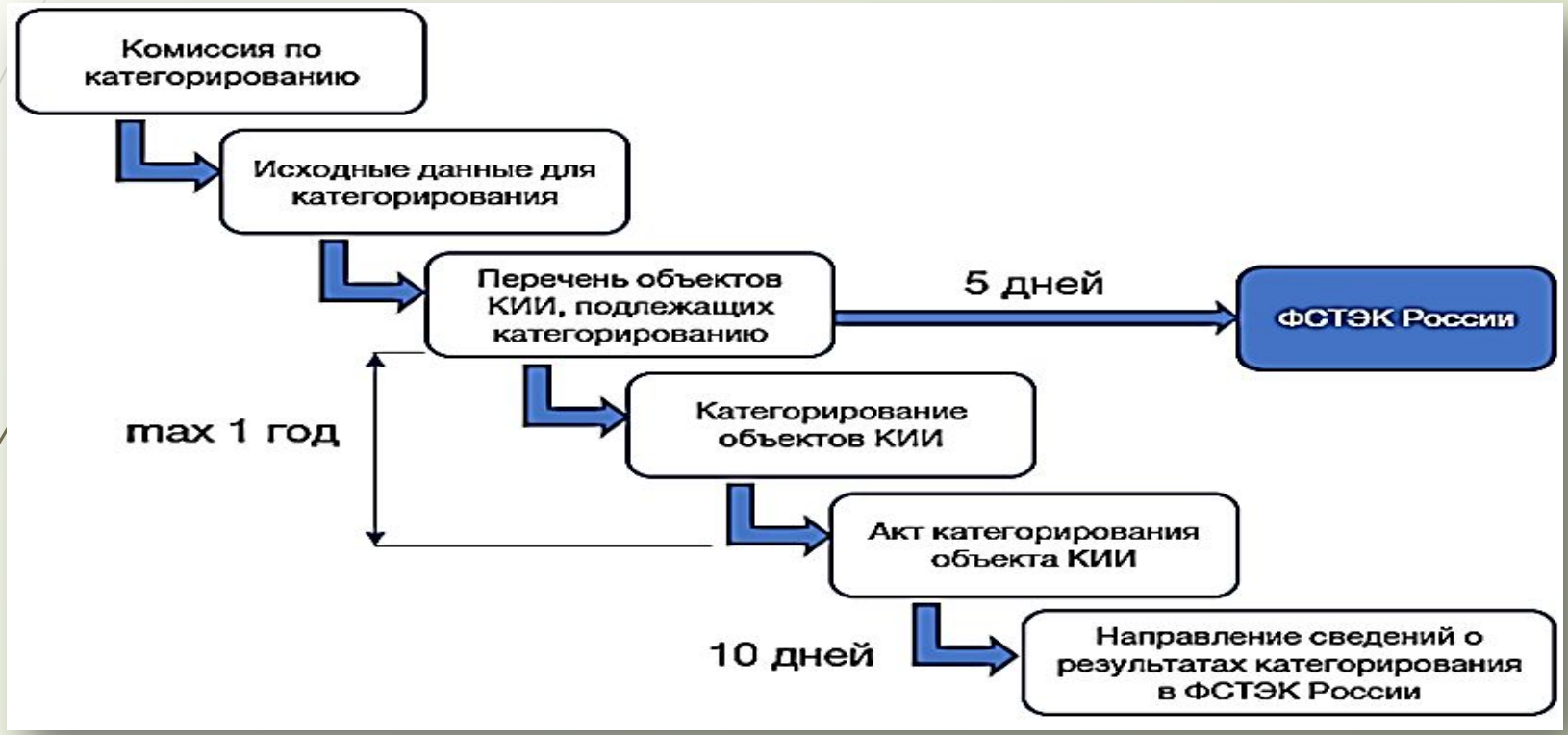
Принцип удовлетворения потребностей при формировании требований к СБО перспективных КИИ

Основывается на следующих предпосылках:

- цели развития СБО КИИ многозначны и не сводятся к единому целевому нормативу, необходимому для формирования критерия оптимальности (целевой функции);
- при обосновании решений математическому описанию доступно ограниченное множество альтернатив, далеко не исчерпывающее всего набора условий и стратегий;
- поиск наиболее рационального решения приходит в условиях ограниченного времени, материальных, финансовых и информационных ресурсов, что не позволяет принимать окончательные решения на ранних стадиях разработки КИИ.

Категорирование объектов КИИ

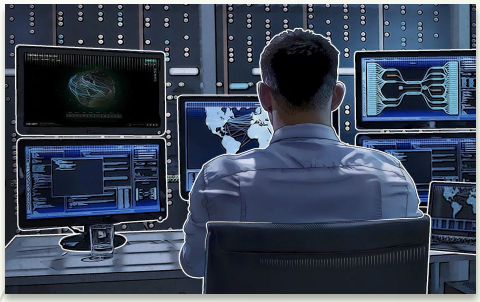
Субъекты КИИ обязаны самостоятельно категорировать принадлежащие им объекты в зависимости от масштаба возможных последствий объекту КИИ.



Процесс категорирования КИИ

Категорирование объектов КИИ осуществляется согласно Постановлению Правительства РФ от 08.02.2018 г. № 127 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

Порядок категорирования объектов КИИ



Субъект КИИ не реже чем один раз в 5 лет осуществляет пересмотр установленной категории значимости и сообщает об изменениях в ФСТЭК.

Изменение категории значимости может произойти:

- По мотивированному решению ФСТЭК по результатам проверки, выполненной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ;
- Объект перестал соответствовать критериям значимости и показателям их значений;
- Субъект КИИ был реорганизован, ликвидирован или произошли изменения в его организационно-правовой форме.

Реестр значимых объектов формируется и ведётся ФСТЭК России на основании данных, предоставляемых субъектами КИИ. Реестр подлежит защите в соответствии законодательством РФ о гос. тайне. Соответствующий документ: **Приказ ФСТЭК от 6.12.2017. № 227**

Требования к системам безопасности значимых объектов КИИ

Система безопасности значимых объектов — это совокупность организационных, технических, правовых и других мер.

Задачи, выполняемые системой безопасности:

1. Предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами;
2. Предотвращение воздействия на технические средства обработки информации, в результате которого может быть нарушено или прекращено функционирование объектов;
3. Восстановление функционирования объектов, если они вышли из строя;
4. Непрерывное взаимодействие с ГОССОПКА.

Приказом ФСТЭК от 21.12.2017 №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

Требования к функционированию системы безопасности значимых объектов КИИ

- Требования к функционированию системы безопасности разделены на 4 этапа, соответствующие классическому циклу PDCA:

1. Планирование и разработка мероприятий
2. Реализация (внедрение) мероприятий
3. Контроль состояния безопасности объектов
4. Совершенствование безопасности объектов

Приказом ФСТЭК от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Реализация требований к ИБ

Включает в себя 5 базовых шагов (приказ №239):

- Шаг 1. Формирование перечня применимых требований
- Шаг 2. Разработка организационных и технических мер.
- Шаг 3. Внедрение организационных и технических мер по обеспечению безопасности.
- Шаг 4. Обеспечение безопасности во время эксплуатации
- Шаг 5. Обеспечение безопасности при выводе из эксплуатации

Ограничения:

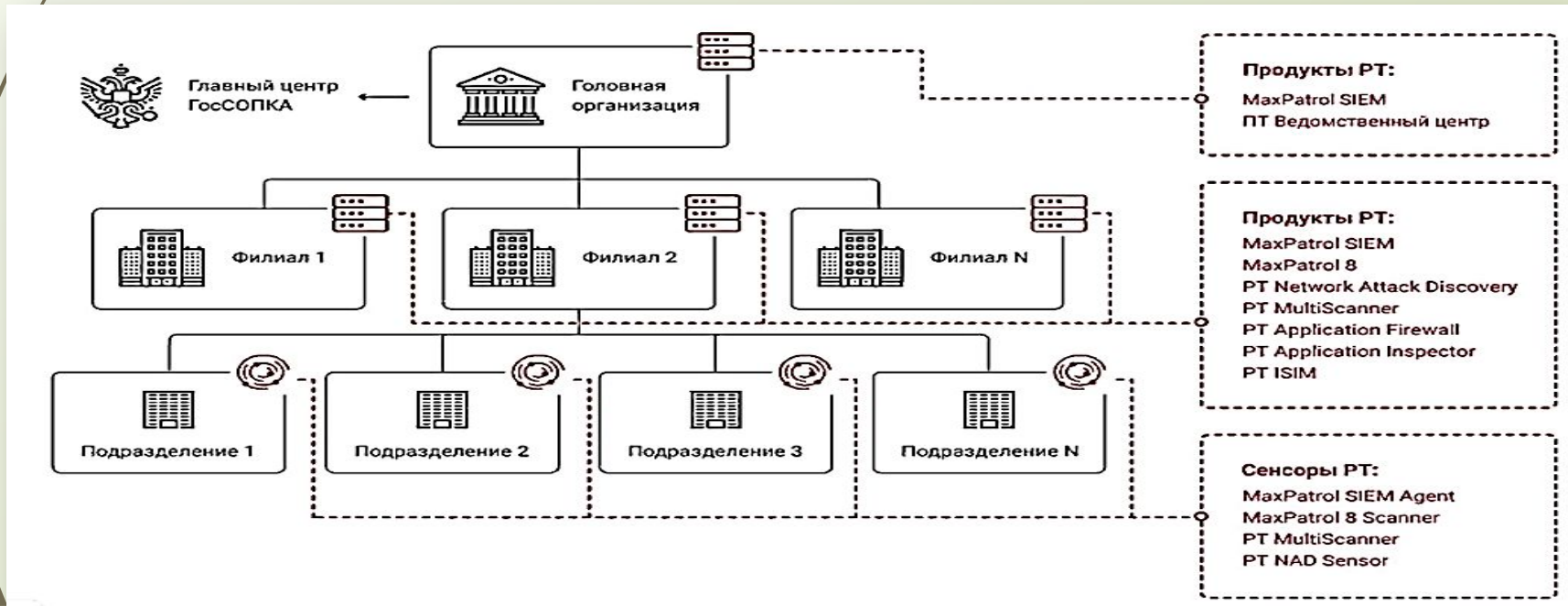
1. Не допускается наличие прямого удаленного доступа к значимому объекту;

2. Не допускается передача информации, в т.ч. технологической, разработчику/производителю значимого объекта без ведома субъекта КИИ.

Категория объекта КИИ	Потенциал источника угроз, который следует рассматривать при выборе мер	Требуемый класс СЗИ
1 категория	Высокий	Не ниже 4 класса
2 категория	Базовый усиленный	Не ниже 5 класса
3 категория	Базовый	Не ниже 6 класса

Совершенствование СБО КИИ с помощью АСУ ТП

1. Единая экосистема продуктов - все продукты интегрируются между собой, что обеспечивает максимальную автоматизацию процессов и упрощает управление информационной безопасностью.
2. Единая техподдержка - техподдержка по всем продуктам оказывается через единое окно.
3. Отечественная разработка - продукты в составе решения включены в реестр российских программ и имеют сертификаты ФСТЭК России .



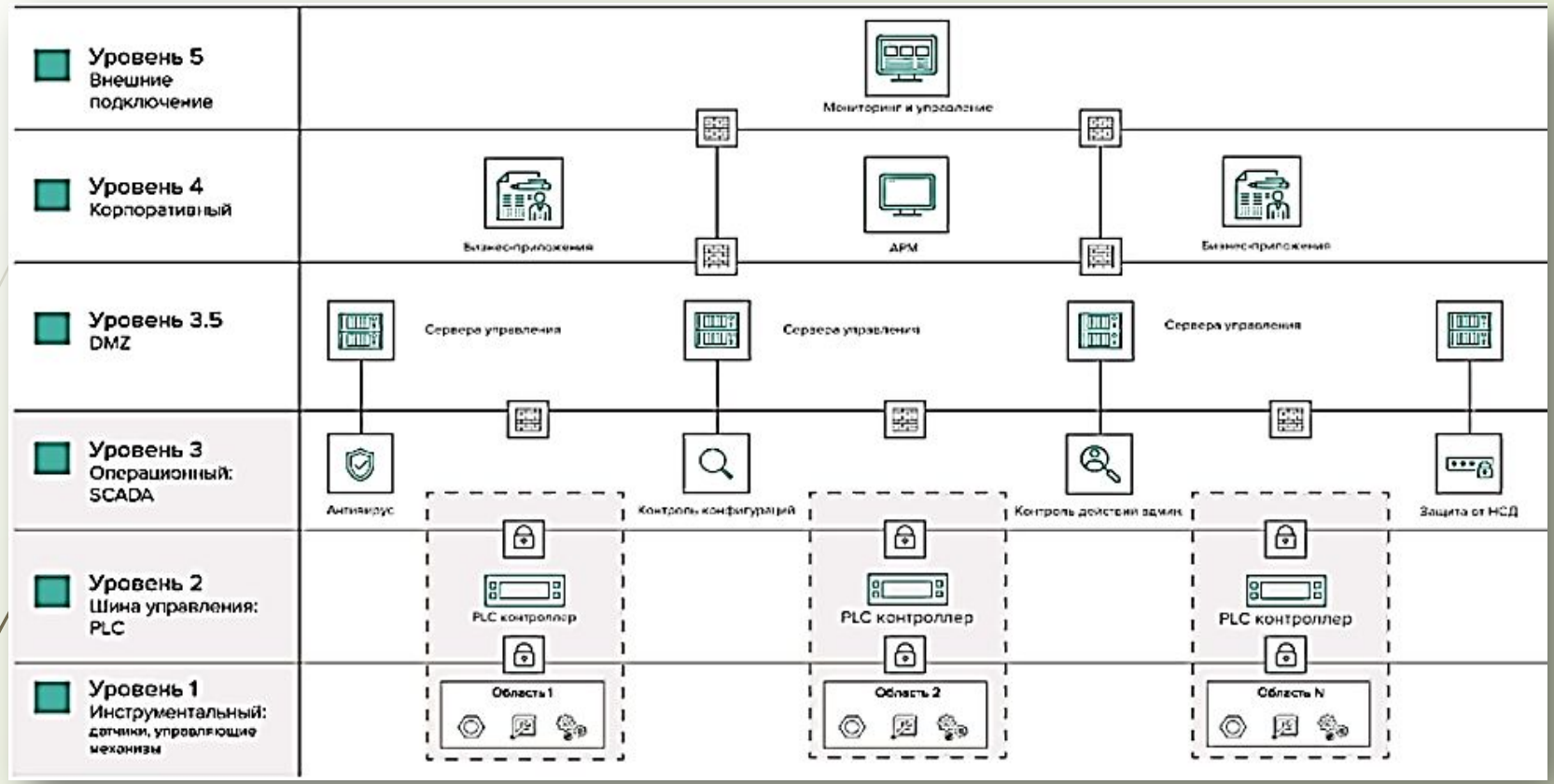
Комплексная система управления ИБ организации

- 03.Security Operation Centre (SOC)
- 02.Positive Technologies MaxPatrol SIEM
- 01. Positive Technologies MaxPatrol.

Состав решения и покрываемые требования

	Приказ ФСТЭК № 235	Приказ ФСТЭК № 239	Приказы ФСБ № 367 и № 368
MaxPatrol 8 — система контроля защищенности и соответствия стандартам ИБ	+	+	—
MaxPatrol SIEM — система мониторинга событий ИБ и выявления инцидентов	+	+	—
PT Network Attack Discovery — система анализа сетевого трафика для выявления и расследования атак	+	+	—
PT MultiScanner — система защиты от вредоносного ПО с «песочницей»	+	+	—
PT Application Firewall — система защиты от веб-атак	+	+	—
PT ISIM — система обнаружения кибератак на АСУ ТП	—	+	—
PT Application Inspector — анализатор защищенности приложений	+	+	—
«ПТ Ведомственный центр» — система управления инцидентами и взаимодействия с ГосСОПКА	—	—	+

Уровни защиты АСУ ТП на КИИ



- На уровне PLC (1уровень) основные векторы атак на уровни PLC – это изменение целостности устройства, перехват, или изменение информации, передаваемой между контроллером и SCADA-серверами.
- Для контроля изменения состояния целостности PLC-контроллера мы предлагаем промышленное решение Kaspersky Industrial Cyber Security for Nodes, которое в режиме реального времени сравнивает контрольные суммы с эталонными значениями и формирует событие информационной безопасности (ИБ) при отклонении.

Выводы

1.Формирование требований представляет собой сложных, динамичный процесс принятия решений в условиях неопределенности исходной информации и ограничений по ресурсам, срокам разработки и ввода в эксплуатацию КИИ.

2. Объекту КИИ присваивается категория значимости, соответствующая наивысшему значению из присвоенных категорий при соотнесении возможного ущерба с показателями категорий значимости.

3. Система защиты АСУ ТП построена на базе платформ отечественных производителей и включает в себя следующие подсистемы:

1. решение для защиты периметра сети,;
2. подсистему управления инцидентами кибербезопасности АСУ ТП и анализа защищенности;
3. подсистему антивирусной защиты;
4. подсистему резервного копирования.

4.В результате возможно снизить риски возникновения инцидентов информационной безопасности, повысить доступность и надежность работы технологических процессов. Немаловажно, что при этом была подготовлена сетевая инфраструктура и платформа информационной безопасности, позволяющая в дальнейшем выполнить требования законодательства в части защиты КИИ – с 1 января 2018 вступил в силу федеральный закон №187-ФЗ «О без-опасности критической информационной инфраструктуры (КИИ)».

Спасибо за внимание!!!