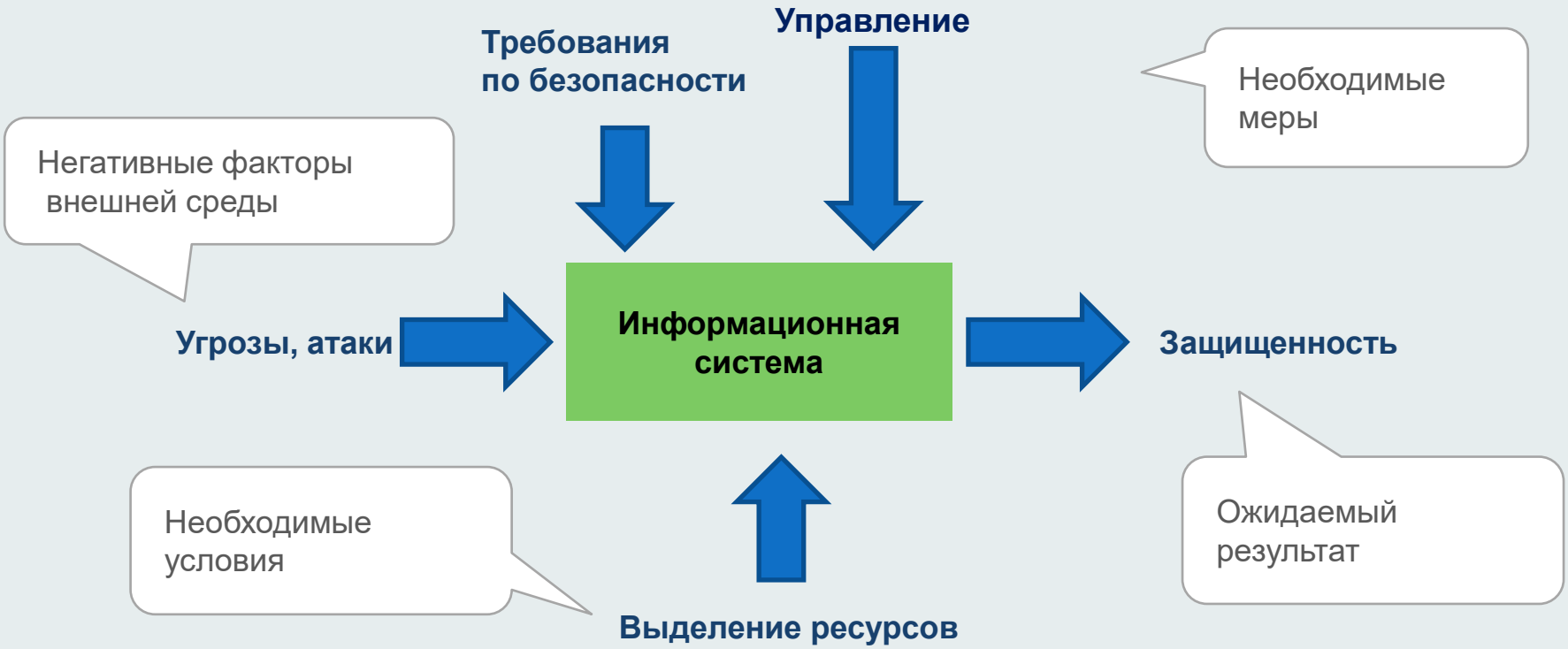
FBK | CS
cybersecurity

Об оценке защищенности информационных систем в современных условиях

Курило А.П.
Советник вице-президента ФБК
по кибер-безопасности, ктн, доцент.

Парадигма защиты



FBK | CS
cybersecurity

О регулировании и управлении

Регулирование: Форма целенаправленного управляющего воздействия, ориентированного на поддержание равновесия в управляемом объекте и на его развитие посредством введения в него регуляторов (норм, правил, целей, связей).

Управление: совокупность процессов, обеспечивающих поддержание системы в заданном состоянии и (или) перевод ее в новое более жизненное состояние организации путем разработки и реализации целенаправленных воздействий.

Выработка управляющих воздействий включает в себя сбор, передачу и обработку необходимой информации, принятие решений, обязательно включающее определение управляющих воздействий.

Контур регулирования «мирного времени»

- **Нормативно-правовое Регулирование;**
- **Техническое регулирование;**
- **Сертификация;**
- **Аттестация;**
- **Аккредитация;**
- **Лицензирование.**

ФСБ

НКЦКИ

ФСТЭК

МИНЦИФРЫ

РКН

Задача регулирования – компенсация возмущений и разрушительных воздействий

FBK | CS cybersecurity

Состав задач регулирования «мирного времени»

Общая цель управления – компенсация возмущений и разрушительных воздействий

Задачи:

1. Поддержание системы безопасности в актуальном состоянии
2. Отражение атак в «фоновом» режиме, когда их интенсивность не слишком высока
3. Мониторинг
4. Плановое развитие и модернизация
5. Соблюдение требований по безопасности на всех этапах жизненного цикла системы
6. Плановые проверки (аудит, оценка соответствия, контрольные мероприятия, тестирование)
7. Тренировки и обучение
8. Менеджмент рисков
9. Киберучения

Управление:

- Директивное
- Оперативное
- Административное
- Инцидентами
- Рисками
- Уязвимостями
- Доступом
- Изменениями
- Персоналом
- Документами

Обратная связь (контроль):

- Аудит
- Оценка соответствия
- Экспресс-оценка защищенности:
- Мониторинг
- Тестирование
- Менеджмент рисков
- Проверки
- Менеджмент инцидентов
- Киберучения

FBK | CS cybersecurity

Состав и цели контрольных мероприятий (в рамках обратной связи системы управления объектом)

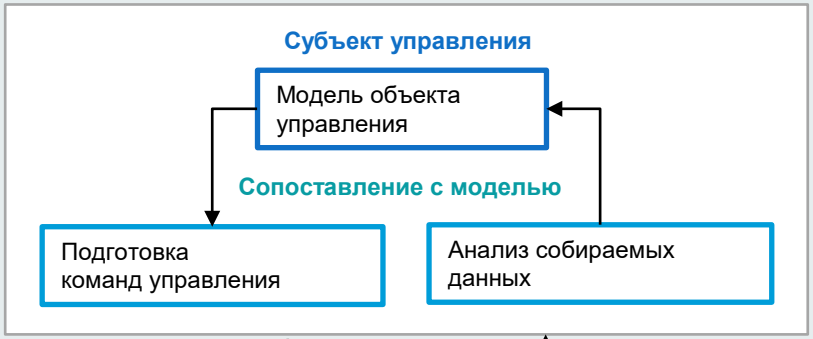
1. **Аудит:** получение объективной и независимой оценки состояния информационной безопасности системы в целом методом опроса и анализа документации (срез «статического состояния системы»;
2. **Оценка соответствия:** получение оценки уровня соответствия требованиям информационной безопасности смешанным методом;
3. **Экспресс-оценка защищенности:** Получение быстрой оценки готовности системы безопасности к отражению наиболее опасных атак, ведущих с возникновению неприемлемого ущерба для активов организации
4. **Мониторинг СОИБ:** постоянное наблюдение и анализ результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей;
5. **Инструментальное тестирование:** получение объективных данных о текущем состоянии обеспечения информационной безопасности корпоративной информационной системы Компании (в том числе от внешних угроз со стороны потенциальных злоумышленников);
6. **Проверка:** проверка работоспособности и подготовленности коллектива;
7. **Менеджмент рисков:** идентификация, количественный и качественный анализ рисков для активов организации с целью их снижения до приемлемого уровня;
8. **Менеджмент инцидентов:** обнаружение и оповещение о возникновении инцидентов, сбор и фиксация информации, связанной с событиями ИБ, оценка, категорирование и реагирование на инциденты, а также и подготовка предложений по устранению причин возникновения инцидентов в будущем;
9. **Киберучения:** практическая проверка готовности системы безопасности противостоять атакам по наиболее вероятным сценариям.

FBK | CS cybersecurity

Сравнительная характеристика эффективности и применимости видов контроля

№ № п/п	Вид контроля	Сфера регули-рования	Регулярность	Нормативная база, требования	% реализации общей задачи защищенности	% эффективности защиты от атак	Что преимуществен-но оценивается
1	**Аудит ИБ**	Общая	Общая- не определено КФС - от 1 до 3 лет	Общая-COBIT КФС- СТО ИББС	До 50	До 20	Статическое состояние
2	**Оценка соответствия требованиям по безопасности**	1. Общая 2. КФС	Общая- не определено КФС - от 1 до 3 лет	1. Общая, по документам ФСТЭК 2. КФС - по ГОСТ	До 70	До 40	Статическое состояние
3	**Экспресс-оценка защищенности**	Общая	Срочная, по указу ПРФ № 250	По оперативным письмам?	5	До 50	Готовность к отражению атак
4	**Инструментальное тестирование**	Общая	Общая- не определено КФС - от 1 до 3 лет Срочная, по указу ПРФ № 250	Общая- не определено КФС - от 1 до 3 лет Срочная, по указу ПРФ № 250	15	До 80	Готовность к отражению атак
5	**Мониторинг СОИБ**	Общая	Требований нет	Не определено	До 10	До 80	Оперативное состояние системы
6	**Контрольная проверка**	Общая	На основании внутренних регламентов	нет	-	-	Подготовленность и работоспособность коллектива
7	**Менеджмент рисков**	КФС	Требований нет	Положение ЦБ, СТО ИББС	3	10	Наличие рисков
8	**Менеджмент инцидентов**	КФС	Требований нет	СТО ИББС	-	-	Готовность к обработке инцидентов
9	**Киберучения**	Общая	Требований нет	нет	-	До 80	Реальная готовность к отражению атак

Контур управления « военного времени»



Управляющее воздействие

Обратная связь

Атаки угрозы

Объект управления (Информационная система)

Состояние защищенности

Ресурсы

- Сбор данных об
- инцидентах
- Оперативные указания
- Контрольные мероприятия

Орган управления Государственной системой защиты информации

ФСБ

НКЦКИ

ФСТЭК

МИНЦИФРЫ

Особенности: резкое усиление ответственности за обеспечение ИБ на местах

FBK | CS cybersecurity

Состав задач управления в условиях «кибервойны»

Главная опасность – прогнозируемый рост интенсивности сложных целевых длительных атак

Цели управления – подготовка к отражению и отражение атак

Главные задачи:

- Экспресс- аудит для выявления основных проблем
- Приведение системы в соответствие рекомендациям регуляторов
- Инструментальное тестирование (на первом этапе-внешнее)
- Полный аудит
- Приведение в соответствие
- Инструментальное тестирование (внешнее, внутреннее)
- Киберучения

Управление:

- Оперативное
- Инцидентами
- Уязвимостями
- Доступом
- Изменениями
- Персоналом

Обратная связь:

- Мониторинг
- Контроль состояния
- Контроль инцидентов;
- Киберучения

FBK | CS cybersecurity

Основная идея: Какие направления атак наиболее опасны, те и нужно защищать в первую очередь.

Что говорят регуляторы

- **НКЦКИ.** Рекомендации по компенсации ИТ-рисков для компаний и организаций Российской Федерации в условиях санкционных ограничений
- **НКЦКИ.** Рекомендации по минимизации возможных угроз информационной безопасности информационным ресурсам Российской Федерации
- **НКЦКИ.** Рекомендации по защите от угроз фишинговых и вредоносных писем
- **НКЦКИ.** Рекомендации по защите информационной инфраструктуры компании от компьютерных атак с использованием программ-шифровальщиков
- **ФСТЭК.** О мерах по повышению защищенности информационной инфраструктуры.
- **ЦБ.** При разработке и реализации мер по обеспечению информационной безопасности участникам обмена рекомендуется применять положения международного стандарта ISO/IEC 27002:2013 Information technology. Security techniques. Codes of practice for information security controls.
- **Минцифры.** Рекомендации по управлению.

FBK | CS cybersecurity

Вопросы контроля и управления

- **Указ Президента РФ №250 от1 мая 2022**
- **Постановление Правительства РФ № 860 от 13 мая 2022 года.**

Основное:

1. Назначить ответственного
2. Создать подразделение
3. Провести независимую проверку
4. Реализовывать требования по безопасности от регуляторов
5. Провести эксперимент

FBK | CS cybersecurity

Этапы работы (желательно 2)

I этап (срочный, по Указу 250):

- Экспресс- аудит для выявления основных проблем
- Приведение системы в соответствие рекомендациям регуляторов
- Внешнее инструментальное тестирование
- Киберучения по сценариям наиболее вероятных атак

II этап (средней срочности, через 2-3 месяца, в плановом порядке:

- Полный аудит, включая оценку соответствия требованиям по информационной безопасности
- Приведение в соответствие по результатам аудита, включая вопросы импортозамещения
- Инструментальное тестирование (внешнее, внутреннее)
- Киберучения по расширенному сценарию, нужно проводить регулярно.

FBK | CS cybersecurity

Суть подхода на первом этапе

(основа - ГОСТ Р ИСО/МЭК 27005 — 2010 Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Менеджмент риска информационной безопасности), раздел 8

1. Идентификация наиболее ценных активов организации
2. Определение неприемлемого ущерба для этих активов
3. Идентификация наиболее вероятных атак, приводящих к возникновению неприемлемого ущерба.
4. Определение наиболее вероятных сценариев реализации этих атак
5. Определение подсистем и элементов информационной системы организации подверженных атакам.
6. Выявление и устранение уязвимостей этих объектов.
7. Тестирование (внутреннее, внешнее)
8. Киберучения по имеющимся сценариям.

Красным выделено авторское дополнение

FBK | CS cybersecurity

О подходах к критериям оценки защищенности (уровня защищенности) объекта

Возможные способы оценки.

1. Качественный (описательный) - акт аудиторской проверки.
2. Количественный:
   a. полнота выполнения всех требований (аттестация объекта защиты, техническое тестирование);
   b. Бальная шкала выполнения требований с выставлением экспертно заданного уровня достаточности (оценка соответствия по ГОСТ Р 57580.2. – 2017)
3. Практический - результат киберучений.

Наиболее подходит комбинированная оценка по п. 2.а и 3.

FBK | CS cybersecurity

FBK | CS
cybersecurity

Спасибо за внимание!

Тел: +7 (495) 737 53 53 доб 3037
Email: Andrey.Kurilo@fbk.ru
Sales@fbkcs.ru