КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КОД ИБ | Челябинск

16.03.2023

- ПОЛИЦКОВОЙ ЕВГЕНИЙ ВИКТОРОВИЧ

_____

ЭКСПЕРТ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА ПРЕДПРИЯТИИ

- Безопасность информации на предприятии

- Непрерывность бизнес-процессов и информационная безопасность

- Управление инцидентами информационной безопасности

Информационная Безопасность - состояние защищенности сбалансированных интересов личности, общества и государства в информационной сфере

Информационная безопасность предприятия - это состояние защищенности от прерываний бизнес процессов в следствии инцидентов информационной безопасности

Обеспечение непрерывности бизнес-процессов и информационной безопасности

Угрозы в сфере информационной безопасности для организации можно подразделить на две категории:

- Внешние
- Внутренние

Защита от утечек информации на предприятии с помощью DLP систем

Data Leak Prevention - предотвращение утечек данных

Построение процесса управления инцидентами

Управление инцидентами – деятельность по восстановлению нормального обслуживания с минимальными задержками и влиянием на бизнес-операции

Стандарты управления инцидентами


ISO/IEC 27001:2013 Information security management system. Requirements

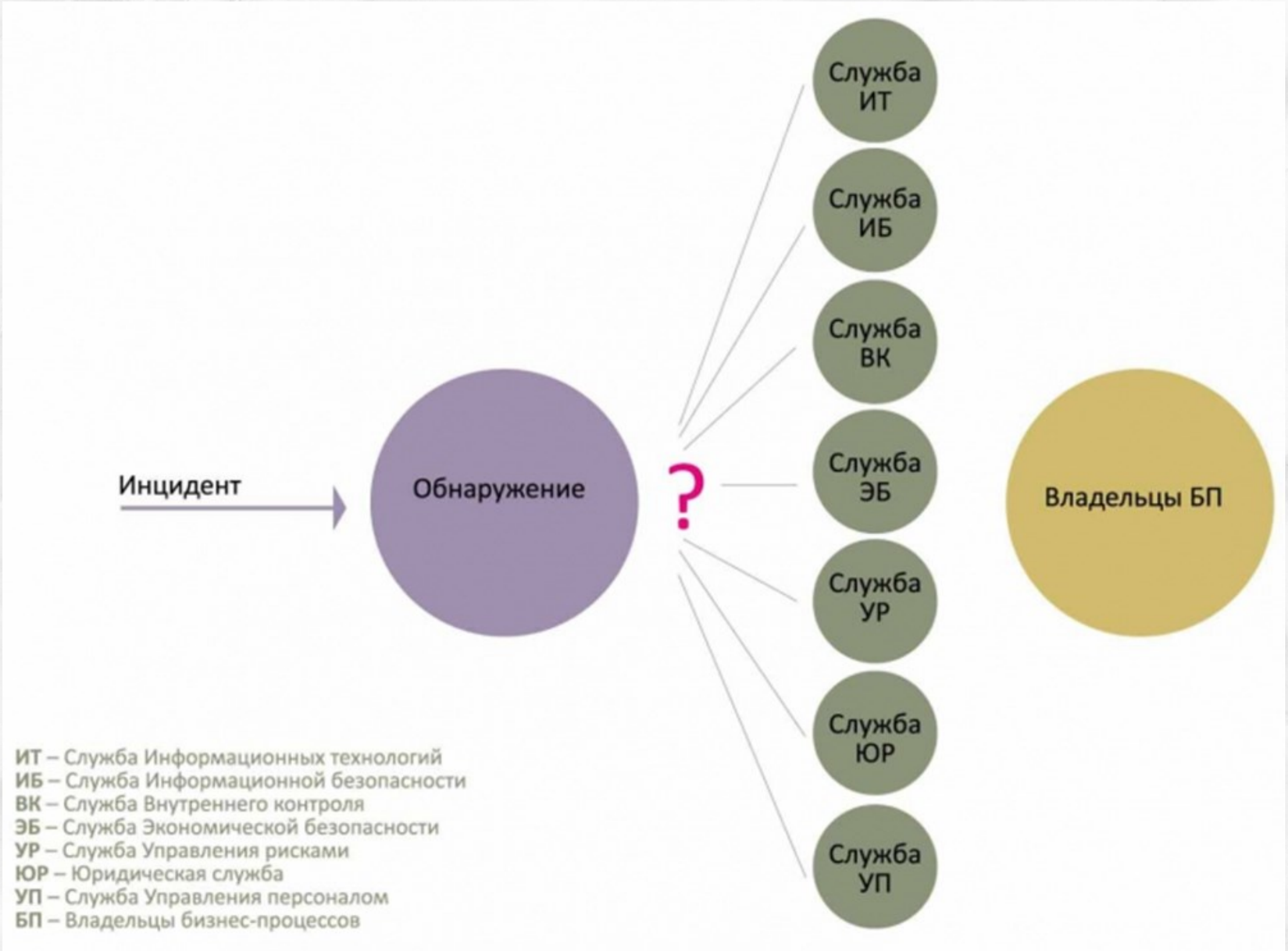

ISO/IEC TR 18044 Information security incident management


CMU/SEI-2004-TR-015 Defining incident management processes for CISRT


NIST SP 800-61 Computer security incident handling guide


ГОСТ Р ИСО/МЭК 18044 Менеджмент инцидентов информационной безопасности

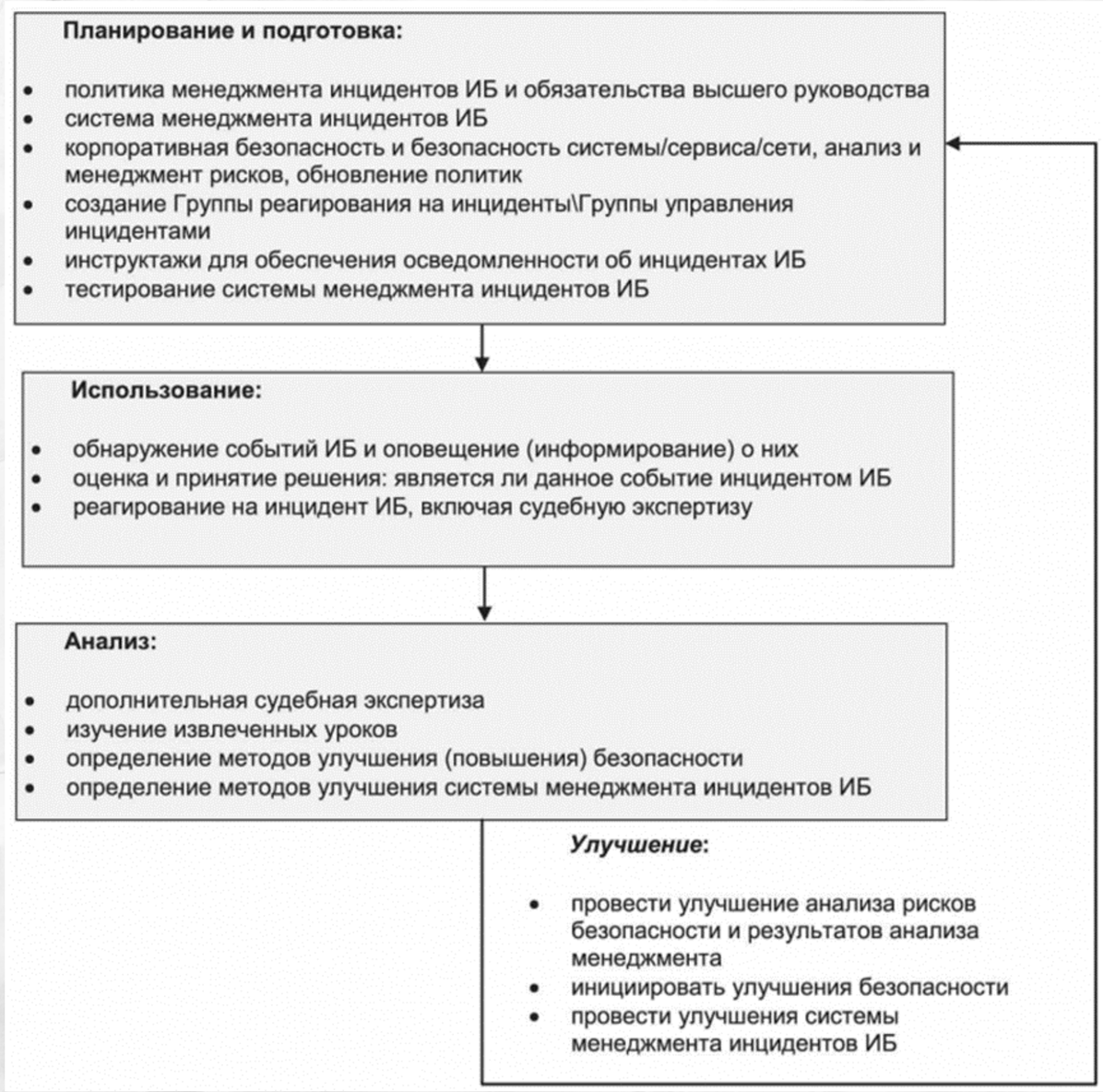
Выявление проблемы



Ключевые цели

1. Быстро обнаружить инцидент
2. Точно идентифицировать инцидент
3. Правильно управлять инцидентом
4. Сдержать инцидент и минимизировать последствия
5. Восстановить сервисы
6. Понять причины
7. Внедрить улучшения для предотвращения повторений

Систематизация работ по реагированию на инциденты



Алгоритм действий менеджера по ИБ

Должности и обязанности

№	Должность	Роль	Обязанности
1.	Комитет по информационной безопасности	Структура, наделенная максимальными полномочиями в области информационной безопасности	1. Ответственность за стратегию управления инцидентами. 2. Утверждение плана управления инцидентами. 3. Согласование исключений и отклонений. 4. Принятие окончательных решений.
2.	Менеджер по информационной безопасности	Руководитель группы по управлению инцидентами и связующее звено с Комитетом по ИБ	1. Разработка, внедрение планов по управлению инцидентами. 2. Эффективное управление рисками и инцидентами. 3. Выполняет про активные и активные меры по контролю уровня информационного риска.
3.	Менеджер по реагированию на инциденты (зачастую, является Менеджером по ИБ)	Руководитель группы реагирования на инциденты	1. Руководство реагированием на инциденты. 2. Координация персонала для эффективного реагирования на инциденты 3. Несёт ответственность за успешное исполнение планов по реагированию на инциденты. 4. Презентация отчета о реагировании на инциденты Комитету по ИБ.
4.	Сотрудник комитете по ИБ	Участие в работе группы	1. Выполняет задачи по минимизации ущерба от инцидента. 2. Документирует шаги, выполняемые в процессе реагирования на инцидент. 3. Сохраняет цепочку доказательств и ведет наблюдение за процессом обработки инцидента в случае судебных разбирательств. 4. Написание отчёта о реагировании на инцидент.

Должности и обязанности , продолжение

№	Должность	Роль	Обязанности
5.	Следователь	Сотрудник Комитета по ИБ	1. Осуществляет расследование инцидента. 2. Находит причину инцидента. 3. Готовит отчет о расследовании.
6.	ИТ специалист по безопасности	Сотрудник Комитета по ИБ, независимый эксперт по ИБ	1. Осуществляет комплексный анализ инцидента с точки зрения ИТ безопасности 2. Осуществляет аудит и самооценку как проактивную меру и часть процесса управления уязвимостями.
7.	Руководители бизнес подразделений	Владельцы бизнес процессов, активов, информационных систем	1. Принимают решения касательно процессов/ресурсов/систем в случае наступления инцидента на основании рекомендаций ГРИГУИ. 2. Проводят первичную оценку влияния угроз на бизнес процессы и определяют приоритет восстановления своих активов.
8.	ИТ специалист	Сотрудник ИТ подразделения	1. Предоставляет помощь в процессе устранения инцидента. 2. Поддерживает информационные системы компании в соответствии с принятыми политиками и правилами.

Должности и обязанности , продолжение

№	Должность	Роль	Обязанности
9.	Юрист	Сотрудник юридического подразделения	Предоставляет помощь в управлении/реагировании/расследовании инцидента при необходимости.
10.	Сотрудник кадровой службы	Специалист по управлению персоналом	1. Предоставляет помощь в управлении/реагировании/расследовании инцидента, когда сотрудник подозревается в его реализации. 2. Встраивает в политику по управлению персоналом аспекты, касающиеся управления инцидентом (санкции для сотрудников, подозреваемых в нарушении политик либо вовлечённых в инцидент).
11.	Пресс-секретарь	Специалист по работе со СМИ и общественностью	Предоставляет подготовленную и необходимую информацию об инциденте акционерам, СМИ и другим с целью сохранения репутации компании и сохранения бренда.
12.	Специалист по анализу рисков	Сотрудник службы ИБ, внутреннего контроля либо управления рисками	1. Вплотную работает с руководителями бизнес подразделений и руководством организации для определения рисков и управления ими. 2. Предоставляет исходные данные (стратегию по управлению рисками) руководству Комитета по ИБ.

Тестирование = Улучшение

Проблемы, влияющие на управление инцидентами

Поддержка — Отсутствие поддержки руководства

— Большинство проблем возникает, если менеджер по ИБ действует самостоятельно, без вовлечения руководства компании и ключевых бизнес-подразделений
— Недостаток встреч и совещаний

Несоответствие — Структура организации не соответствует ее целям

— Бизнес работает в ускоренном темпе и может значительно измениться в течение короткого периода времени. Процесс управления инцидентами может быть не в состоянии справиться со скоростью и характером изменений, происходящих в организации. Руководство, как правило, занимается бизнес вопросами и может быть не в состоянии тратить время на управление инцидентами. Определить какие-либо критические ошибки и довести их до руководства компании является ответственностью менеджера по ИБ.

Текучка — Частая смена членов ГРИ

— Разработка плана управления инцидентами может занять значительное количество времени при постоянном взаимодействии с различными заинтересованными сторонами. Руководитель ГРИ, как правило, либо член руководства или менеджер по ИБ, может неожиданно покинуть компанию, в результате чего реализация планов или совершенствование процесса может быть остановлено. В таком случае совершенствование управления инцидентами может перейти на второй план.

Общение — Недостаток коммуникационного процесса

— Может привести к различного рода непониманию о необходимости управления инцидентами, планирования, тестирования.

Сложность — Сложность плана по управлению инцидентами

— Предлагаемый план может быть хорошим и охватывать многие вопросы, но это может оказаться слишком сложным для восприятия. Те, кому он предназначен могут его не понять и как следствие – выполнение будет невозможным.

Принципы работы с инцидентами

- Безопасность сотрудников и посетителей;
- Сдерживание инцидента и минимизация ущерба;
- Безопасность активов организации;
- Безопасность информационных ресурсов;
- Восстановление в соответствии с требованиями бизнеса;
- Расследование инцидента;
- Принятие мер по недопущению повторения инцидента.

Готов ответить
на ваши вопросы

Спасибо за внимание!