УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ от А до Я

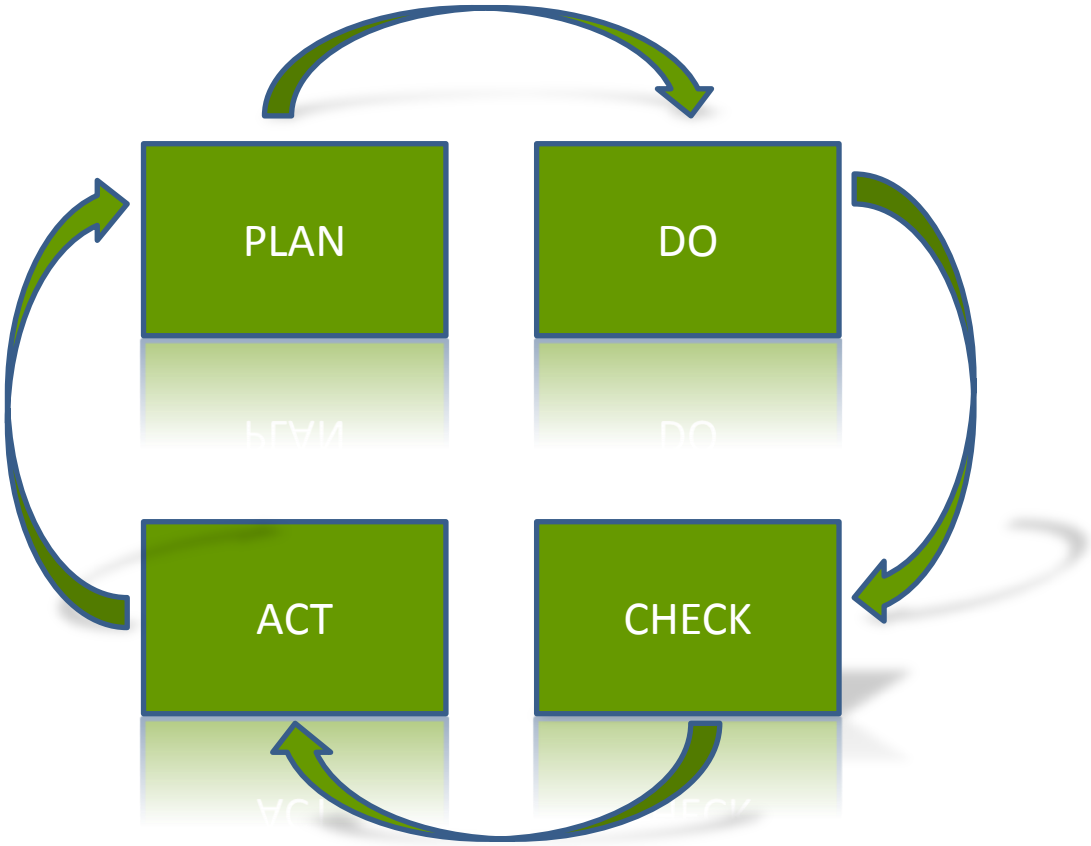
Ксения Засецкая
Старший консультант Отдела консалтинга
АО «ДиалогНаука»

ДиалогНаука

План вебинара

- ✓ Управление инцидентами. Ключевые этапы создания и внедрения процесса
- ✓ Классификация инцидентов. Необходимое и достаточное количество классификационных параметров
- ✓ Выявление инцидентов. Достаточно ли SIEM?
- ✓ Обработка инцидентов информационной безопасности
- ✓ Расследование инцидентов
- ✓ Оценка эффективности процесса управления инцидентами информационной безопасности

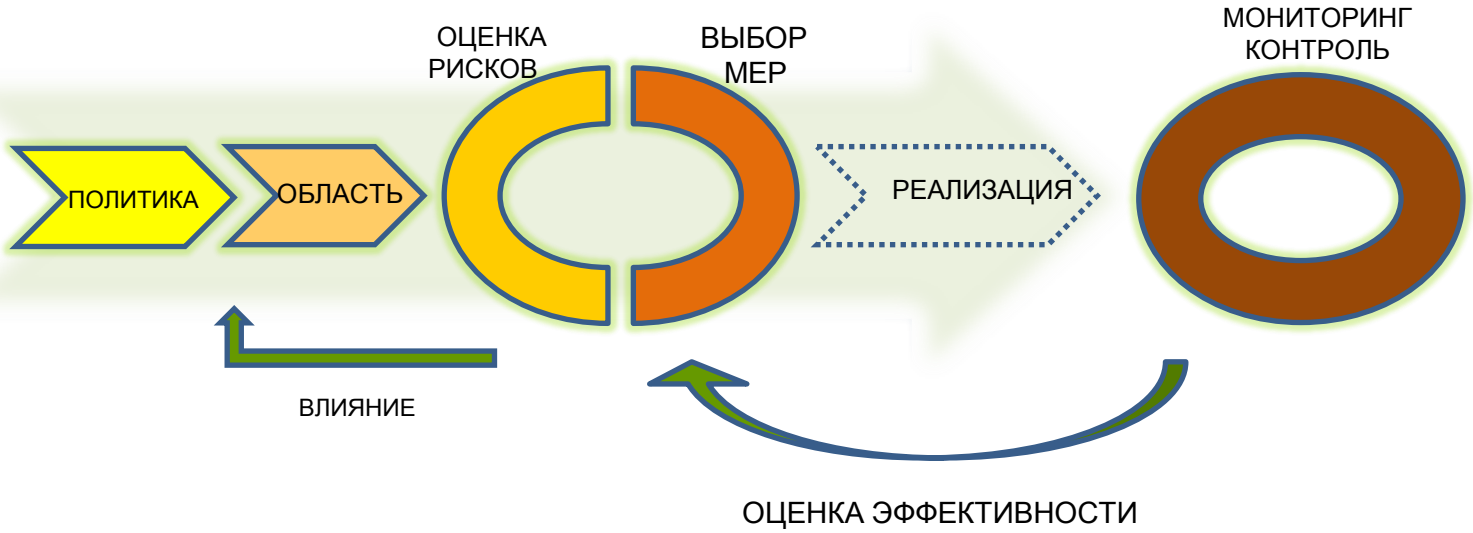
Управление инцидентами



Для описания процессов управления инцидентами безопасности используется классическая модель непрерывного улучшения процессов - PDCA (Plan — Do — Check — Act).

Управление инцидентами

Основные этапы реализации процесса управления инцидентами



События и инциденты

Инцидент информационной безопасности

One or multiple related and identified information security events that can harm an organization's assets or compromise its operations

(ISO/IEC 27035-1:2016)

Событие ИБ или их комбинация, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:

- нарушение в СОИБ организации БС РФ, включая нарушение работы средств защиты информации;
- нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов организации БС РФ в области обеспечения ИБ, нарушение в выполнении процессов СМИБ организации БС РФ;
- нарушение в выполнении банковских технологических процессов организации БС РФ;
- нанесение ущерба организации БС РФ и (или) ее клиентам

(БР ИББС 2.5-2014)

- ✓ События ИБ – не всегда инциденты. События могут указывать на возможные нарушения информационной безопасности или ошибки контроля
- ✓ Необходимо определить **критерии** отнесения событий информационной безопасности к инцидентам

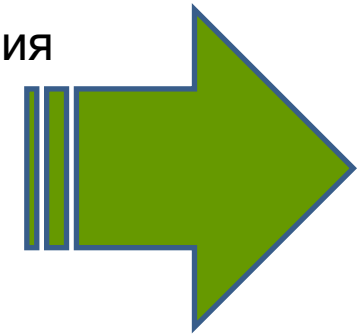
Классификация инцидентов

Для чего необходима классификация инцидентов:

- ✓ Приоритезация (определения приоритета обработки инцидентов ИБ)
- ✓ Последствия (определения влияния и возможных последствий инцидента ИБ)
- ✓ Минимизация (определения оптимального способа дальнейшей обработки)
- ✓ Статистика (анализа произошедших инцидентов ИБ, подведения статистики)

Классификационные признаки

- ✓ Категория
- ✓ Тип
- ✓ Критичность
- ✓ Характер воздействия
- ✓ Масштаб
- ✓ Негативные последствия
  Приоритет
- ✓ Длительность
- ✓ Время
- ✓ Источник информации
- ✓ Способ обнаружения
- ✓ Информационная система
- ✓ Бизнес-процесс
- ✓ Результат
- ✓ Намеренность
- ✓ Сложность
- ✓ и другие



Необходимо разделить все классификационные признаки на группы в зависимости от стадии обработки инцидента:

- ✓ Первичные
- ✓ Уточняющие
- ✓ Информационные
- ✓ Результирующие

Классификационные признаки

- Категория
- Тип
- Критичность
- Источник

Первичные

- Средство защиты информации
- Правило (сценарий)
- Возможность негативных последствий и их тип
- Уровень эскалации
- Информационная система
- Тип информации

Уточняющие

- Намеренность
- Масштаб

Информационные

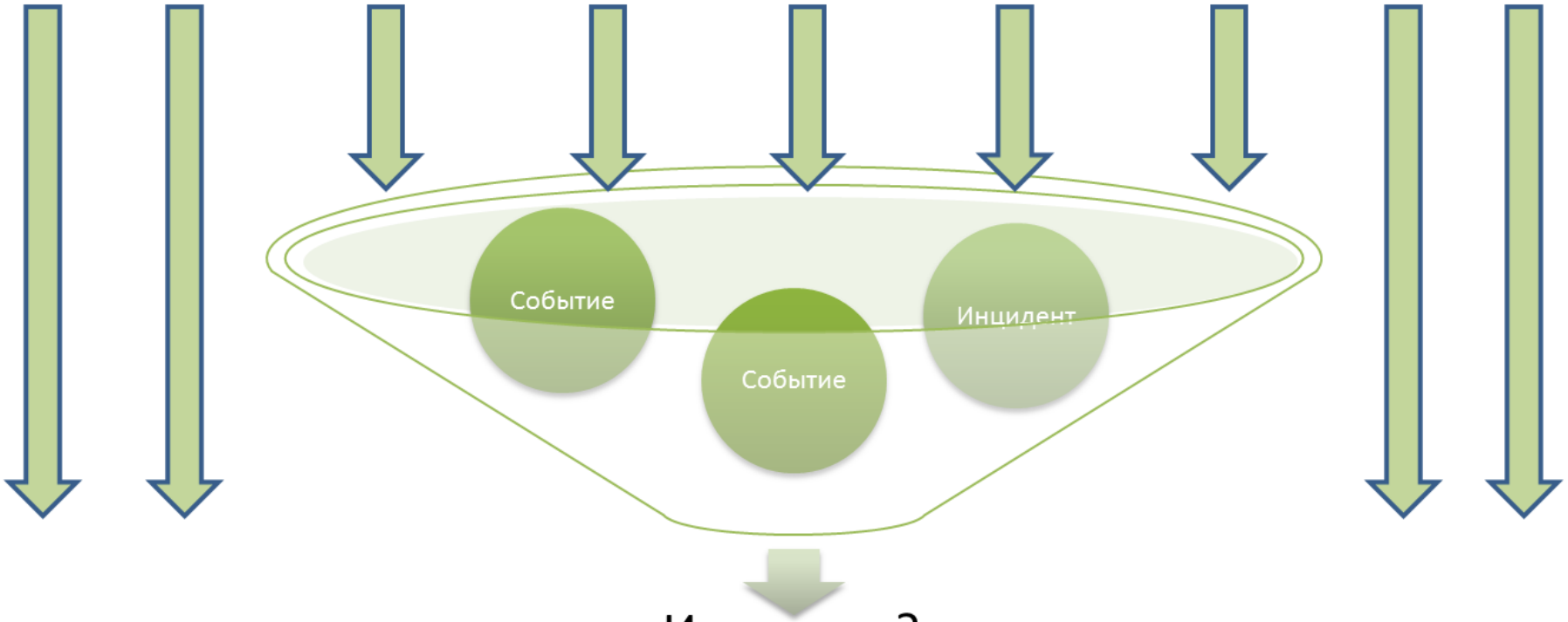
- Сложность обнаружения
- Повторяемость
- Степень вероятности повторного возникновения

Результирующие

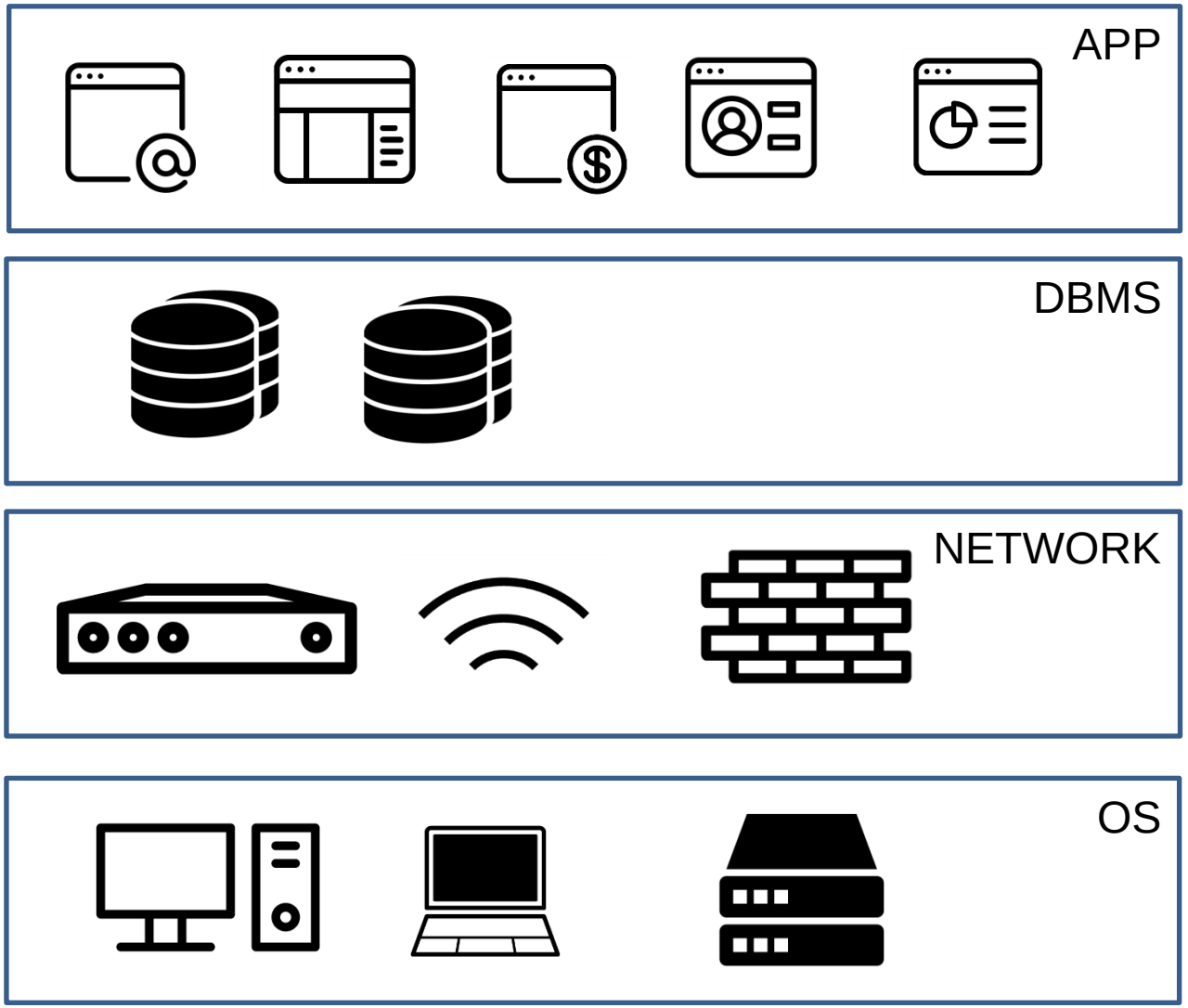
Выявление инцидентов

Основные источники информации о потенциальных инцидентах:

- ✓ пользователи
- ✓ информационные системы
- ✓ компоненты ИТ-инфраструктуры
- ✓ средства защиты информации
- ✓ клиенты
- ✓ контрагенты
- ✓ внешние сервисы

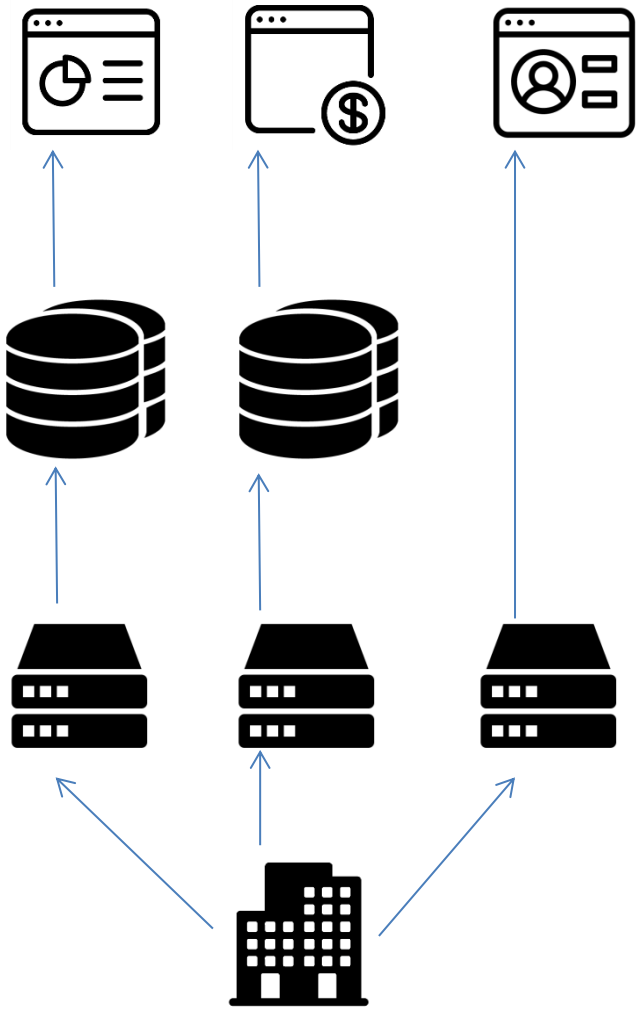


Выявление инцидентов



Для эффективного выявления инцидентов необходимо собирать и анализировать события ИБ на всех уровнях среды обработки защищаемой информации.

Выявление инцидентов



Если в Компании:

- ✓ используется CMDB
- ✓ описана сервисно-ресурсная модель информационных систем

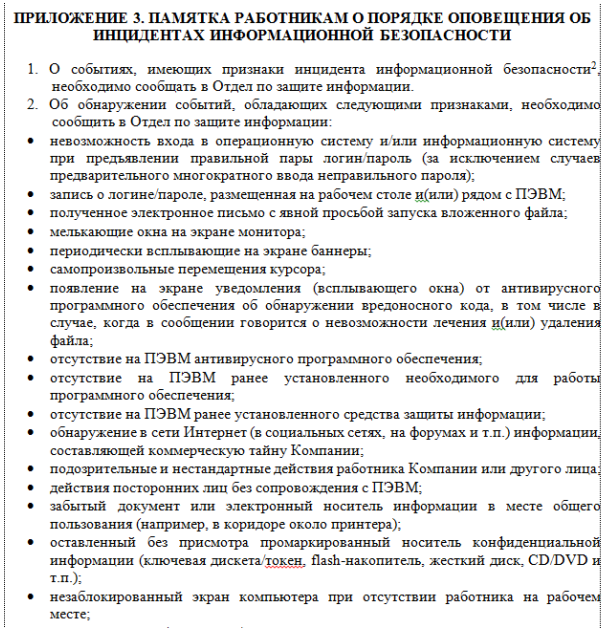
то возможна разработка комплексный сценариев выявления инцидентов ИБ

Важно! Необходима привязка к реальным бизнес-процессам с целью минимизации последствий для основной деятельности Компании!

Выявление инцидентов

Необходимо проводить регулярное повышение осведомленности персонала в вопросах обеспечения информационной безопасности и оповещения о потенциальных инцидентах:

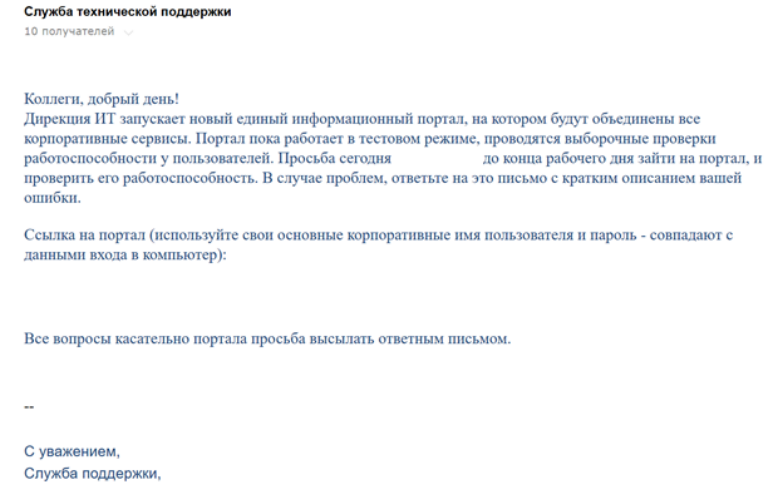
- ✓ Разработка памятки
- ✓ Проведение обучающих семинаров
- ✓ Тренинги (например, в форме тестирования на проникновение по модели «Black box»).



ПРИЛОЖЕНИЕ 3. ПАМЯТКА РАБОТНИКАМ О ПОРЯДКЕ ОПОВЕЩЕНИЯ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. О событиях, имеющих признаки инцидента информационной безопасности[2], необходимо сообщать в Отдел по защите информации.
2. Об обнаружении событий, обладающих следующими признаками, необходимо сообщить в Отдел по защите информации:

- невозможность входа в операционную систему и/или информационную систему при предъявлении правильной пары логин/пароль (за исключением случаев предварительного многократного ввода неправильного пароля);
- запись о логине/пароле, размещенная на рабочем столе и(или) рядом с ПЭВМ;
- полученное электронное письмо с явной просьбой запуска вложенного файла;
- мелькающие окна на экране монитора;
- периодически всплывающие на экране баннеры;
- самопроизвольные перемещения курсора;
- появление на экране уведомления (всплывающего окна) от антивирусного программного обеспечения об обнаружении вредоносного кода, в том числе в случае, когда в сообщении говорится о невозможности лечения и(или) удаления файла;
- отсутствие на ПЭВМ антивирусного программного обеспечения;
- отсутствие на ПЭВМ ранее установленного необходимого для работы программного обеспечения;
- отсутствие на ПЭВМ ранее установленного средства защиты информации;
- обнаружение в сети Интернет (в социальных сетях, на форумах и т.п.) информации, составляющей коммерческую тайну Компании;
- подозрительные и нестандартные действия работника Компании или другого лица;
- действия посторонних лиц без сопровождения с ПЭВМ;
- забытый документ или электронный носитель информации в месте общего пользования (например, в коридоре около принтера);
- оставленный без присмотра промаркированный носитель конфиденциальной информации (ключевая дискета/токен, flash-накопитель, жесткий диск, CD/DVD и т.п.);
- незаблокированный экран компьютера при отсутствии работника на рабочем месте;



Служба технической поддержки

10 получателей

Коллеги, добрый день!
Дирекция ИТ запускает новый единый информационный портал, на котором будут объединены все корпоративные сервисы. Портал пока работает в тестовом режиме, проводятся выборочные проверки работоспособности у пользователей. Просьба сегодня до конца рабочего дня зайти на портал, и проверить его работоспособность. В случае проблем, ответьте на это письмо с кратким описанием вашей ошибки.

Ссылка на портал (используйте свои основные корпоративные имя пользователя и пароль - совпадают с данными входа в компьютер):

Все вопросы касательно портала просьба высылать ответным письмом.

--

С уважением,
Служба поддержки,

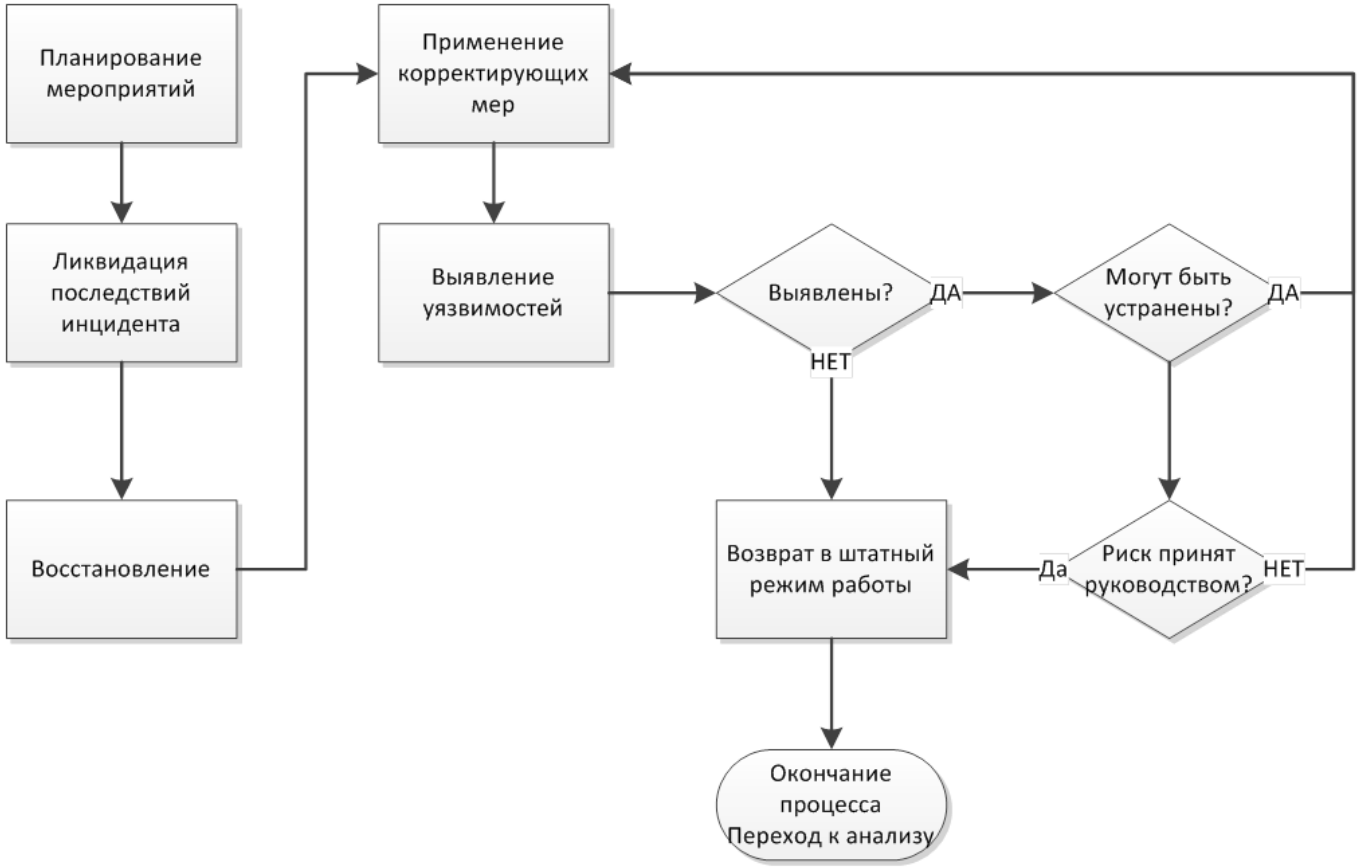
Первичное реагирование

- ✓ **Важно!** При реагировании необходимо стремиться к минимальному промежутку времени между выявлением инцидента и реагированием на него

- ✓ Аналитический процесс – второй этап, зачастую длительный.

Обработка инцидента

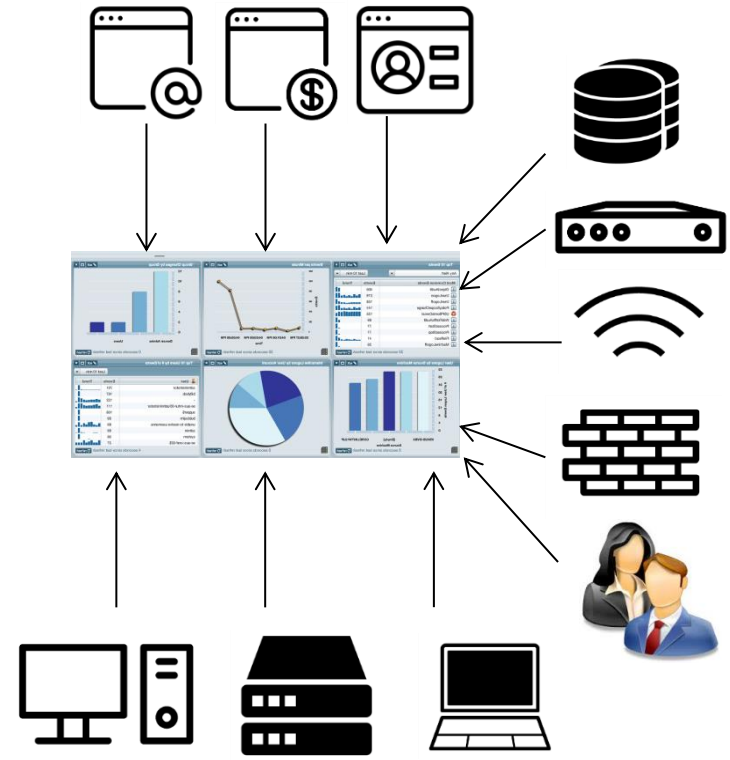
Принятие решения о последующих действиях может быть реализовано по следующему принципу:



Источники информации

- ✓ Необходимы отлаженные и известные всей команде Ситуационного центра способы взаимодействия с другими внутренними подразделениями организации (управление безопасности, инженеры безопасности, администраторы, управление кадрами, юристы, связи с общественностью, бизнес-подразделения) и, в случае необходимости, с внешними организациями (специалистами по расследованию инцидентов, внешние сервисы, правоохранительные органы, ФСБ, ФСТЭК и т.д.)

Ведение учета инцидентов ИБ



- ✓ Регистрация всех инцидентов
- ✓ Единая система
- ✓ Контроль жизненного цикла
- ✓ Возможность корреляции
- ✓ Ретроспективный анализ

Расследование инцидентов

С целью развития процессов расследования инцидентов ИБ и формирования доказательной базы должны быть выполнены следующие основные действия:

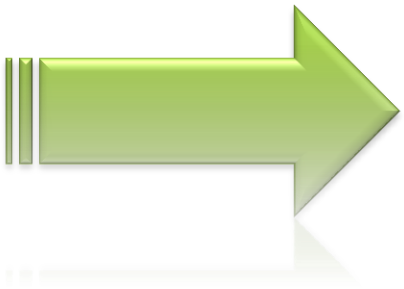
1. Определить и описать типы инцидентов (сценарии), требующие формирования доказательной базы.
2. Определить доступные источники и типы информации, которая может использоваться в качестве доказательной базы.
3. Определить требования к сбору доказательств с этих источников.
4. Организовать возможность для корректного (с юридической точки зрения) сбора доказательной базы в соответствии с определенными требованиями.
5. Установить политику хранения и использования (обработки) потенциальных доказательств.
6. Обеспечить мониторинг событий, указывающих на инцидент ИБ
7. Определить события, при наступлении которых должны быть запущены процессы сбора доказательной базы (указать это в типовых планах)
8. Описать все роли в рамках данного процесса и провести необходимое обучение вовлеченных работников.
9. Описать основные планы реагирования на инциденты, требующие сбора доказательной базы (юридически значимой).
10. Обеспечить правовую экспертизу.

Криминалистика

- ✓ Forensic (форензика) – компьютерная криминалистика - наука о раскрытии и расследовании преступлений, связанных с компьютерной информацией, о методах получения и исследования цифровых доказательств, о применяемых для этого технических средствах
- ✓ Обеспечение целостности и неоспоримости процесса при расследовании
- ✓ Формы участия в расследовании:
  - Компьютерно-технические экспертизы
  - Участие в следственных действиях
  - Участие в проведении оперативно-розыскных мероприятиях
  - Участие в судебных заседаниях
  - Использование специализированных технических средств
  - Обучение специалистов внутри организации

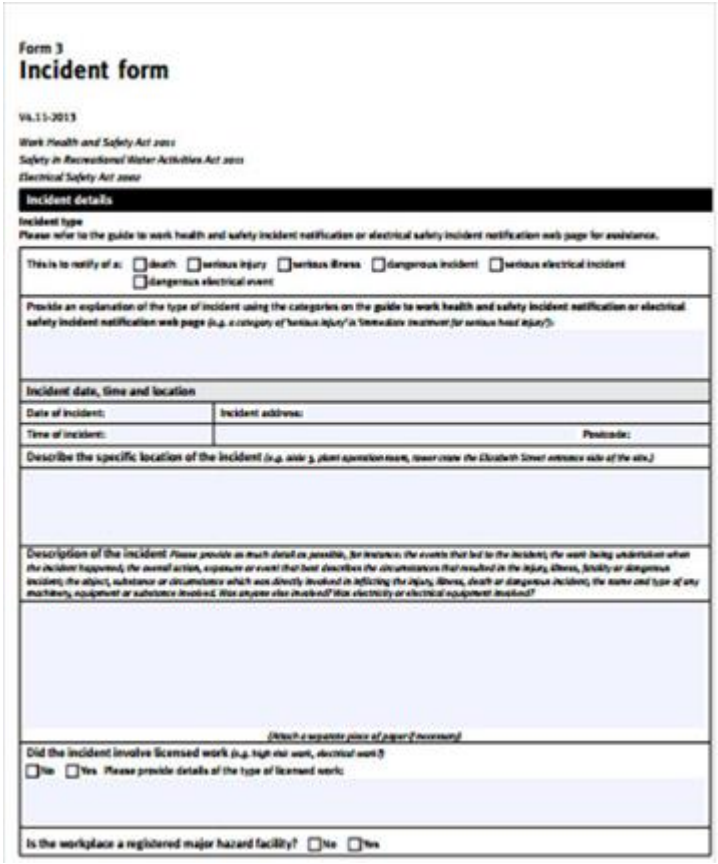
Криминалистика

- ✓ Определение необходимого объема
- ✓ Инструктаж всех пользователей
- ✓ Возможно ли реализовать своими силами или же надо привлекать специалистов
- ✓ Определение порядка сбора и хранения



- Формирование и утверждение процедур
- Выбор технических средств
- Информирование пользователей
- Реализация процесса

«Жизнь» инцидента



Form 3

Incident form

v4.11-2013

Work Health and Safety Act 2011
Safety in Recreational Water Activities Act 2011
Electrical Safety Act 2002

Incident details

Incident type

Please refer to the guide to work health and safety incident notification or electrical safety incident notification web page for assistance.

This is to notify of a: ☐ death ☐ serious injury ☐ serious illness ☐ dangerous incident ☐ serious electrical incident ☐ dangerous electrical event

Provide an explanation of the type of incident using the categories on the guide to work health and safety incident notification or electrical safety incident notification web page (e.g. a category of 'serious injury' is 'immediate treatment for serious head injury'):

Incident date, time and location

Date of incident:	Incident address:
Time of incident:	Postcode:

Describe the specific location of the incident (e.g. aisle 3, plant operation room, tower crane the Elizabeth Street entrance side of the site.)

Description of the incident: Please provide as much detail as possible, for instance the events that led to the incident, the work being undertaken when the incident happened, the overall action, exposure or event that best describes the circumstances that resulted in the injury, illness, fatality or dangerous incident, the object, substance or circumstance which was directly involved in inflicting the injury, illness, death or dangerous incident, the name and type of any machinery, equipment or substance involved. Was anyone else involved? Was electricity or electrical equipment involved?

(Attach a separate piece of paper if necessary)

Did the incident involve licensed work (e.g. high risk work, electrical work)?

☐ No ☐ Yes Please provide details of the type of licensed work:

Is the workplace a registered major hazard facility? ☐ No ☐ Yes

Обработка инцидентов

Пример плана реагирования на инцидент определенного типа: «Компрометация учетной записи»

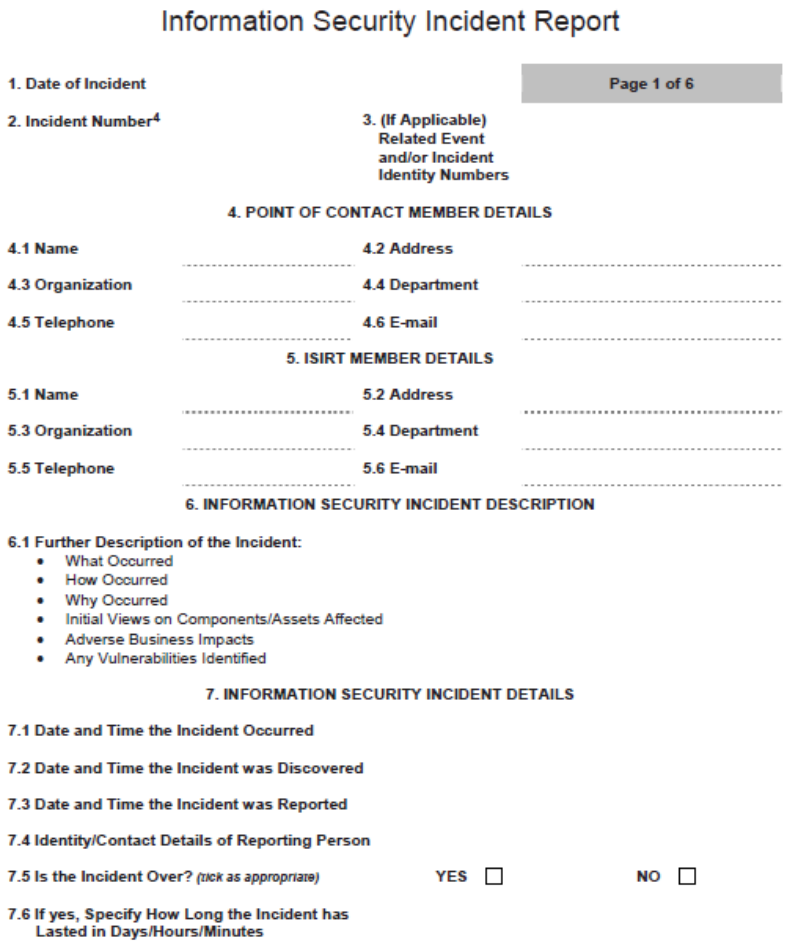
№	Этап	Вход	Действия	Выход	Ответственный	Срок
1	Обнаружение	Инцидент ИБ (тип: Компрометация учетной записи)	Информирование Администратора АС/Администратора AD	-	Оператор системы мониторинга	5 мин
2	Блокирование	Учетная запись АС/AD	Блокирование учетной записи	-	Администратор АС/Администратор AD	
3	Расследование	Журналы регистрации событий ИБ	Выявление фактов несанкционированного использования учетной записи (изучение данных регистрации)	Информация об использовании учетной записи Информация о действиях злоумышленника Последствия инцидента ИБ	Администратор АБС/Администратор AD	
4	Создание новой учетной записи	-	Активация новой учетной записи (смена пароля учетной записи)		Администратор АС/Администратор AD	

Отчет по результатам обработки инцидента

- ✓ Для кого?
- ✓ С какой целью?
- ✓ Какое наполнение?

Отчет может содержать:

- ✓ основные сведения
- ✓ информацию об объекте инцидента
- ✓ информацию об источнике инцидента
- ✓ описание хронологии инцидента
- ✓ принятые меры по реагированию
- ✓ решение по инциденту
- ✓ информацию о вовлеченных лицах



Information Security Incident Report

1. Date of Incident — Page 1 of 6

2. Incident Number[4]

3. (If Applicable) Related Event and/or Incident Identity Numbers

4. POINT OF CONTACT MEMBER DETAILS

4.1 Name ..... 4.2 Address .....

4.3 Organization ..... 4.4 Department .....

4.5 Telephone ..... 4.6 E-mail .....

5. ISIRT MEMBER DETAILS

5.1 Name ..... 5.2 Address .....

5.3 Organization ..... 5.4 Department .....

5.5 Telephone ..... 5.6 E-mail .....

6. INFORMATION SECURITY INCIDENT DESCRIPTION

6.1 Further Description of the Incident:

- What Occurred
- How Occurred
- Why Occurred
- Initial Views on Components/Assets Affected
- Adverse Business Impacts
- Any Vulnerabilities Identified

7. INFORMATION SECURITY INCIDENT DETAILS

7.1 Date and Time the Incident Occurred

7.2 Date and Time the Incident was Discovered

7.3 Date and Time the Incident was Reported

7.4 Identity/Contact Details of Reporting Person

7.5 Is the Incident Over? *(tick as appropriate)* YES ☐ NO ☐

7.6 If yes, Specify How Long the Incident has Lasted in Days/Hours/Minutes

Анализ процесса

- ✓ Почему произошел инцидент?
- ✓ Есть ли другие инциденты, вызванные исходной причиной?
- ✓ Участники инцидента?
- ✓ Что нужно изменить?
- ✓ Что можно изменить?
- ✓ Что делать дальше?

Оценка эффективности процессов

Оценка эффективности процесса управления инцидентами ИБ направлена на корректировку (совершенствование):

- ✓ процесса управления инцидентами;
- ✓ реализованных мер обеспечения ИБ;
- ✓ подхода и результатов оценки рисков;
- ✓ области мониторинга и контроля;
- ✓ политики (подходов).

Оценка эффективности

Оценка эффективности должна быть направлена на следующие основные области процесса управления инцидентами:

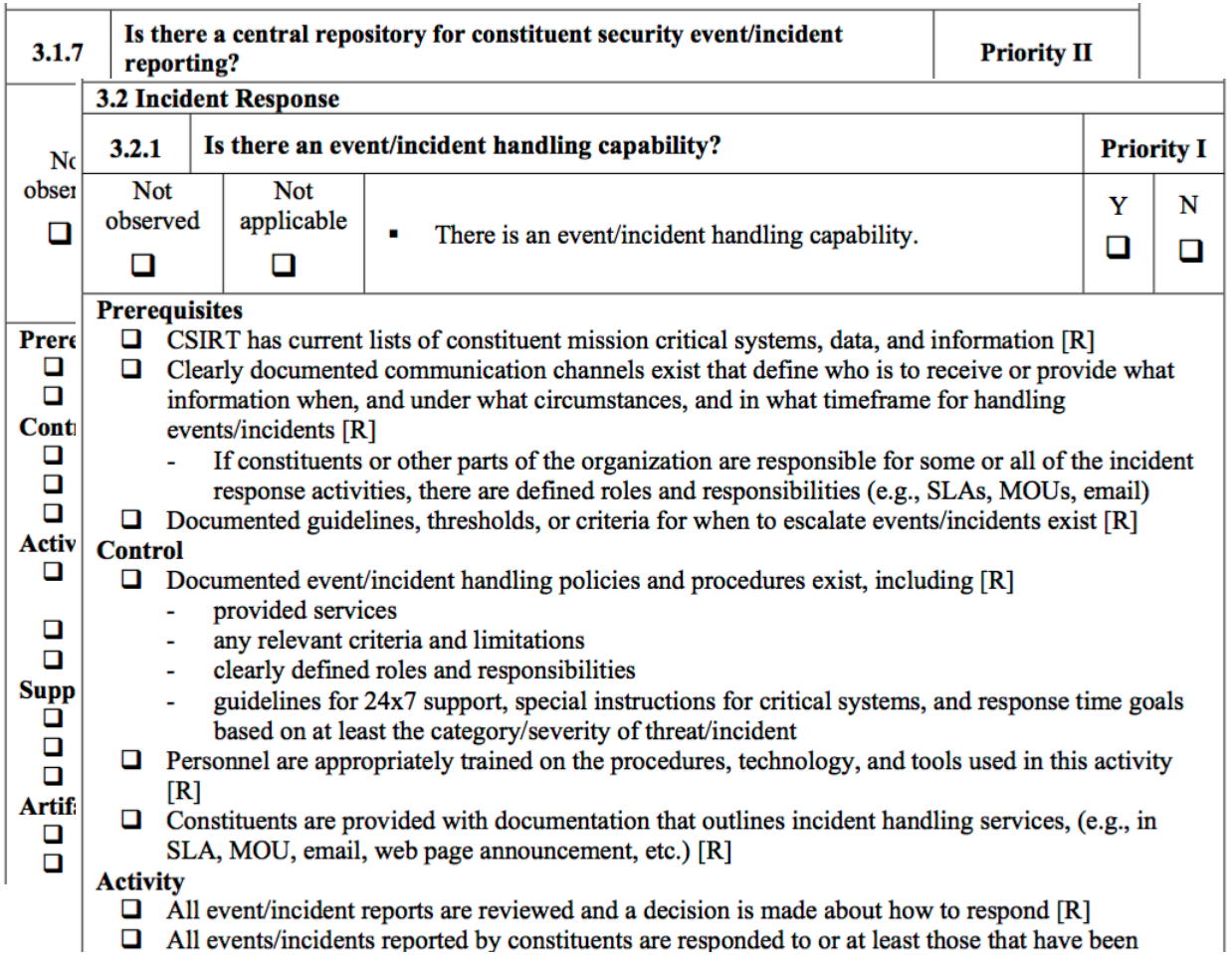
- ✓ общие требования и подход к управлению инцидентами
- ✓ защита информации (превентивные меры)
- ✓ выявление инцидентов
- ✓ обработка инцидентов
- ✓ принятие решений по инцидентам

В каждой области должны быть сформированы свои оценочные показатели.

Оценка эффективности

Критерии для формирования метрик:

- ✓ ISO/IEC 270XX
- ✓ SANS Institute
- ✓ CERT
- ✓ NIST
- ✓ рекомендации и документация разработчиков SIEM (HPE, IBM)



3.1.7	**Is there a central repository for constituent security event/incident reporting?**	**Priority II**

3.2 Incident Response

3.2.1	**Is there an event/incident handling capability?**				**Priority I**
Not observed ❑	Not applicable ❑	▪ There is an event/incident handling capability.		Y ❑	N ❑

Prerequisites

- ❑ CSIRT has current lists of constituent mission critical systems, data, and information [R]
- ❑ Clearly documented communication channels exist that define who is to receive or provide what information when, and under what circumstances, and in what timeframe for handling events/incidents [R]
  - If constituents or other parts of the organization are responsible for some or all of the incident response activities, there are defined roles and responsibilities (e.g., SLAs, MOUs, email)
- ❑ Documented guidelines, thresholds, or criteria for when to escalate events/incidents exist [R]

Control

- ❑ Documented event/incident handling policies and procedures exist, including [R]
  - provided services
  - any relevant criteria and limitations
  - clearly defined roles and responsibilities
  - guidelines for 24x7 support, special instructions for critical systems, and response time goals based on at least the category/severity of threat/incident
- ❑ Personnel are appropriately trained on the procedures, technology, and tools used in this activity [R]
- ❑ Constituents are provided with documentation that outlines incident handling services, (e.g., in SLA, MOU, email, web page announcement, etc.) [R]

Activity

- ❑ All event/incident reports are reviewed and a decision is made about how to respond [R]
- ❑ All events/incidents reported by constituents are responded to or at least those that have been

Спасибо за внимание!

Вопросы?

АО «ДиалогНаука»

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru

e-mail: k.zasetskaya@DialogNauka.ru