# Администрирование информационных систем

Смирнов Михаил
СПбГУ
2009

- доступность (возможность за приемлемое время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного ознакомления).

# Основные хар-ки информации

# Целостность

- различные аспекты целостности курируют ФАПСИ и Гостехкомиссия.
- Целостность можно подразделить на:
  - статическую (понимаемую как неизменность информационных объектов). Под нее в основном все регламенты
  - динамическую (относящуюся к корректному выполнению сложных действий (транзакций)).
    - Пример области применения средств контроля динамической целостности — анализ потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

# Конфиденциальность

- Конфиденциальность — самый проработанный у нас в стране аспект информационной безопасности.
- На страже конфиденциальности стоят законы, нормативные акты, многолетний опыт соответствующих служб.
- Отечественные аппаратно-программные продукты позволяют закрыть практически все потенциальные каналы утечки информации.
- Но и эта часть далека он полного охвата. Есть ограничения и на быстродействие аппаратуры. И на внедрение в ПО

- Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:
  - законодательного (законы, нормативные акты, стандарты и т.п.);
  - административного (действия общего характера, предпринимаемые руководством организации);
  - процедурного (конкретные меры безопасности, имеющие дело с людьми);
  - программно-технического (конкретные технические меры).

# *Конфиденциальность*

# Методология оценки риска.

- Оценка риска является первым процессом в методологии управления рисками.
- Результаты этого процесса помогают идентифицировать соответствующие меры по управлению (контролю) за сокращением или устранением риска
- Чтобы определить вероятность будущего неблагоприятного события, потенциальные угрозы для ИТ-систем должны быть одновременно проанализированы с двух позиций:
  - потенциальной уязвимости
  - наличия средств контроля (управления) в соответствующем месте ИТ-системы.
- Воздействие риска выражается степенью вреда, который мог бы быть вызван осуществлением данной угрозы для данного вида уязвимости.

| Исходные данные | | Действия по оценке риска | | Результаты |
|---|---|---|---|---|
| 1. • Компьютерное оборудование<br>2. • Программное обеспечение<br>3. • Системные интерфейсы<br>4. • Данные и информация<br>5. • Люди<br>6. • Миссия системы | | **Шаг 1**<br>**Характеристика системы** | | 1. • Границы системы<br>2. • Функции системы<br>3. • Критичность системы и данных<br>4. • Чувствительность системы и данных |
| 1. • История атак на систему<br>2. • Данные от разведывательных агентств, NIPC, OIG, FedCIRC, СМИ | | **Шаг 2**<br>**Идентификация угроз** | | 1. • Формулировки угроз |
| 1. • Отчеты по предыдущим оценкам рисков<br>2. • Сообщения о различных аудитах<br>3. • Требования к безопасности<br>4. • Результаты тестирования безопасности | | **Шаг 3**<br>**Идентификация уязвимости** | | 1. • Перечень потенциальных точек уязвимости |

# Схема оценки риска – 1

| | | | | |
|---|---|---|---|---|
| 1.• Текущее состояние контроля<br>2.• Планируемые мероприятия по контролю | | **Шаг 4**<br>**Анализ контроля (управления)** | | 1.• Перечень текущих и планируемых мер по проведению контроля |
| 1.• Мотивация источников угроз<br>2.• Возможности угроз<br>3.• Природа уязвимости<br>4.• Текущее состояние контроля | | **Шаг 5**<br>**Определение вероятности (возможности)** | | 1.• Рейтинги возможности осуществления угроз |
| 1.• Анализ воздействия на выполнение миссии<br>2.• Оценка критичности активов<br>3.• Критичность данных<br>4.• Чувствительность данных | | **Шаг 6**<br>**Анализ воздействия** | | 1.• Рейтинги воздействия угроз |

# Схема оценки риска– 2

| | | | | |
|---|---|---|---|---|
| 1.• Вероятность угрозы для эксплуатации<br>2.• Размеры воздействия<br>3.• Адекватность планируемых или текущих мер по контролю | | **Шаг 7**<br>**Определение риска** | | 1.• Риски и уровни допустимых рисков |
| | | **Шаг 8**<br>**Рекомендации по контролю** | | 1.• Рекомендованные мероприятия по контролю |
| | | **Шаг 9**<br>**Документальное оформление результатов** | | 1.• Отчет по оценке рисков |

# Схема оценки риска– 3

| Источник и угрозы | Мотивации | Угрожающие действия |
|---|---|---|
| Хакеры, взломщики | 1. • Вызовы<br>2. • Эгоцентризм, самомнение<br>3. • Бунт, противодействие | 1. • хакерство<br>2. • социальная разработка (Social engineering)<br>3. • вторжение или проникновение в систему<br>4. • несанкционированный доступ к системе |
| Компьютерные преступники | 1. • Разрушение информации<br>2. • Незаконное раскрытие информации<br>3. • Денежно-кредитные операции с целью получить выгоду<br>4. • Несанкционированное изменение данных | 1. • компьютерное преступление (например, киберпреследование)<br>2. • мошеннический акт (например, переигрывание, имитирование или перехват)<br>3. • информационное взяточничество<br>4. • получение доступа путем обмана<br>5. • вторжение в систему |

# Классификация возможных угроз со стороны людей -1

| | | |
|---|---|---|
| Террористы | 1. • Шантаж<br>2. • Разрушение<br>3. • Эксплуатация<br>4. • Месть | 1. • терроризм<br>2. • информационная война<br>3. • нападение на системы (например, невозможность распределенного обслуживания)<br>4. • проникновение в систему<br>5. • вмешательство в систему |
| Промышленный шпионаж (компании, иностранные правительства, интерес со стороны других правительственных ведомств) | 1. • Получение конкурентоспособных преимуществ<br>2. • Экономический шпионаж | 1. • экономическая эксплуатация<br>2. • кража информации<br>3. • покушение на секретность персональных данных<br>4. • социальная разработка<br>5. • проникновение в систему<br>6. • несанкционированный доступ в систему |

# Классификация возможных угроз со стороны людей -2

| | | |
|---|---|---|
| Посвященные в систему люди (плохо обученные, обозленные, рассерженные, злонамеренные, небрежные, нечестные или уволенные служащие) | 1. • Любопытство<br>2. • Эгоцентризм<br>3. • Получение данных<br>4. • Денежно-кредитные устремления<br>5. • Месть<br>6. • Неумышленные ошибки и упущения (например, ввод ошибочных данных, ошибка программирования) | 1. • просмотр конфиденциальной внутренней информации<br>2. • злоупотребление компьютером<br>3. • мошенничество и воровство<br>4. • информационное взяточничество<br>5. • ввод фальсифицированных, искаженных данных<br>6. • перехват данных<br>7. • ввод злонамеренных кодов (например, вирусов, логических бомб, троянских коней)<br>8. • продажа персональной информации<br>9. • внесение дефектов в систему<br>10. • вторжение в систему<br>11. • создание саботажа со стороны системы<br>12. • несанкционированный доступ в систему |

# Классификация возможных угроз со стороны людей -3

| Уязвимость | Источник угрозы | Угрожающее действие |
|---|---|---|
| Системные идентификаторы уволенных служащих не удалены из системы. | Уволенные служащие | Вхождение в сеть компании и доступ к данным, которые являются собственностью компании. |
| Брандмауэр компания позволяет идентифицированным гостям через средства сетевого теледоступа вхождение на XYZ сервер. | Неавторизованные пользователи (например, хакеры, уволенные служащие, компьютерные преступники, террористы) | Использование сетевого теледоступа к XYZ серверу идентифицированными гостями. |
| Производитель идентифицировал существующие недостатки в системе безопасности, однако, новые решения не применены в системе. | Неавторизованные пользователи (например, хакеры, уволенные служащие, компьютерные преступники, террористы) | Получение несанкционированного доступа к чувствительным файлам системы, благодаря известным точкам уязвимости системы. |

# примеры пар: уязвимость / угроза

| Уровень возможности | Определение |
| --- | --- |
| Высокий | Источник угрозы является высокоактивным и обладает достаточно высокими возможностями, в то время как управление предотвращением использования уязвимости для осуществления этой угрозы оказывается неэффективным. |
| Средний | Источник угрозы является достаточно активным и способным, однако средства управления, находящиеся на местах и обязанные воспрепятствовать использованию уязвимости действуют эффективно и могут противостоять угрозе. |
| Низкий | У источника угроз отсутствуют мотивации для осуществления угроз или они очень незначительны, а средства управления, находящиеся на местах, имеют возможность эффективно препятствовать использованию уязвимости для осуществления угроз. |

# Вероятности угрозы

| Уровень возможности | Определение |
|---|---|
| Высокий | Реализация угрозы через существующую в системе уязвимость:<br>1) может окончиться серьезными потерями дорогостоящих основных материальных активов или ресурсов;<br>2) может значительно нарушить, повредить или воспрепятствовать выполнению миссии организации, нанести вред репутации организации или ее интересам;<br>3) может закончиться человеческими жертвами или серьезным материальным ущербом. |
| Средний | Реализация угрозы через существующую в системе уязвимость:<br>1) может окончиться дорогостоящими потерями материальных активов или ресурсов;<br>2) может нарушить, повредить или воспрепятствовать выполнению миссии организации или нанести вред ее репутации или ее интересам;<br>3) может окончиться ущербом для людей. |
| Низкий | Реализация угрозы через существующую в системе уязвимость:<br>1) может окончиться потерей некоторых материальных активов или ресурсов;<br>2) может заметно затрагивать процесс выполнения миссии организации или ее репутацию и интересы. |

# Воздействие угрозы

- может быть выражено в виде следующих метрик:
  - Вероятность того, что данный источник  угрозы попытается использовать и успешно преодолеет данную уязвимость;
  - Величина воздействия, которое может возникнуть, если  источник угрозы успешно использует данную уязвимость;
  - Адекватность запланированной или существующей системы безопасности для сокращения или устранения риска.

# Определение риска для любой конкретной пары угроза / уязвимость

# Уменьшение рисков.

- ***Принятие риска (Risk Assumption).***
  - *Принимать потенциальный риск, либо реализовать средства управления, позволяющее снизить риск до приемлемого уровня.*
- ***Предотвращение риска (Risk Avoidance).***
  - *Избегать рисков, устраняя причину риска и/или его последствия.*
- ***Ограничение риска (Risk Limitation).***
  - *Ограничивать имеющийся риск, реализовав и применив средства управления, которые минимизируют неблагоприятное воздействие осуществления угрозы для уязвимости.*
- ***Планирование риска (Risk Planning).***
  - *Управлять риском, путем разработки плана действий по уменьшению риска, который может предусматривать введение определенных приоритетов, реализацию и проведение контроля.*
- ***Исследование и уведомление (Research and Acknowledgment).***
  - *Понизить риск возможных потерь, путем уведомления о наличии уязвимости или недостатков в системе и исследования средств контроля для исправления уязвимости.*
- ***Перенос риска (Risk Transference).***
  - *Переместить риск, используя другие опции, чтобы получить компенсации за возможные потери, например, путем страхования покупок.*

- Определение воздействия осуществления новых или проведения усовершенствования  существующих средств управления;
- Определение воздействия не осуществления нового или не проведения усовершенствования  существующих средств управления
- Оценка затрат на выполнения перечисленных действий:
  - закупки аппаратных средств ЭВМ и программного обеспечения,
  - снижение эксплуатационной эффективности, если характеристики системы или ее функциональные возможности будут уменьшены для увеличения безопасности,
  - затраты на осуществление дополнительных видов политики и процедур,
  - затраты на прием дополнительного персонала служащих, которые должны будут осуществлять предложенную политику, процедуры или услуги,
  - затраты на обучение персонала,
  - затраты на поддержание и на обслуживание.
- Оценка рентабельности реализации по сравнению с критичностью системы и данных
- Риск, остающийся после реализации нового средства управления или проведения усовершенствования существующего средства управления является остаточным риском

# Анализ рентабельности и остаточный риск

- работа с пользователями:
  - создание и удаление пользовательских бюджетов (учетных записей), их блокировка и разблокирование,
  - настройка сценариев входа,
  - консультирование пользователей по различным аспектам работы с системой и нахождению тех или иных ресурсов.
- управление данными
  - Предоставление пользователям прав на доступ к конкретным ресурсам,
  - профилактическое обслуживание баз данных (индексация, оптимизация, упаковка),
  - организация резервного копирования.
- Анализ производительности и оптимизация системы.
- учет системных ресурсов.
  - контроль использования дискового пространства, печати,
  - учет трафика.

# основные компоненты администрирования крупных информационных систем -1

- Техническое обслуживание и модернизация.
- Управление активным сетевым оборудованием и сетью в целом.
- Обеспечение информационной безопасности:
  - составление плана доступа пользователей к ресурсам (в соответствии с принятой в компании политикой информационной безопасности)
  - контроль его исполнения.
  - отслеживание появления различных уязвимостей в используемых операционных системах,
  - организация получения и установки "заплаток" (patches).
- Аудит

# основные компоненты администрирования крупных информационных систем -2

- Администратор 1. Оптимизация настроек. Мониторинг производительности. Модернизация. Техническое обслуживание и профилактика. Организация резервного копирования.
- Администратор 2. Регистрация новых пользователей. Отслеживание изменения статуса пользователей (ведение и хранение учетных карт). Консультация пользователей. Смена и восстановление пароля, решение других проблем.
- Администратор 3. Организация размещения данных. Назначение/изменение прав доступа. Планирование резервного копирования и хранение резервных копий. Восстановление данных (совместно с администратором 1).
- Администратор безопасности системы. Участие в разработке матрицы доступа к ресурсам. Контроль за соблюдением политики безопасности при эксплуатации. Отслеживание информации об уязвимостях системы и своевременное принятие мер. Периодическое практическое тестирование защищенности системы.
- Аудитор. Настройка подсистемы регистрации. Организация архивирования и хранения журналов регистрации. Анализ журналов регистрации.

# 5 категорий административного персонала