

Информационная безопасность организации

Урок 1.

**Что такое информационная безопасность и
почему ею стоит заниматься?**

Лысяк Александр

<http://inforsec.ru>

Безопасность

- **ИБ** – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.
- **Защита информации** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Безопасность информации

- это *состояние* защищённости информационной среды,
- *защита информации* представляет собой *деятельность* по предотвращению несанкционированных, преднамеренных и непреднамеренных воздействий на защищаемую информацию и поддерживающую инфраструктуру
- то есть *процесс*, направленный на достижение этого состояния.



Основные задачи ЗИ

- Обеспечение следующих характеристик:
 - Целостность
 - Доступность
 - Конфиденциальность
 - Подотчетность
 - Аутентичность
 - Достоверность

По ГОСТ 133335-4. Методы и средства обеспечения безопасности



Целостность

- Актуальность и непротиворечивость информации, её защищённость от разрушения и несанкционированного изменения.



- Типы целостности:
 - Статическая (неизменность ИО)
 - Динамическая (корректное выполнение сложных транзакций).

Доступность



- Состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

Конфиденциальность



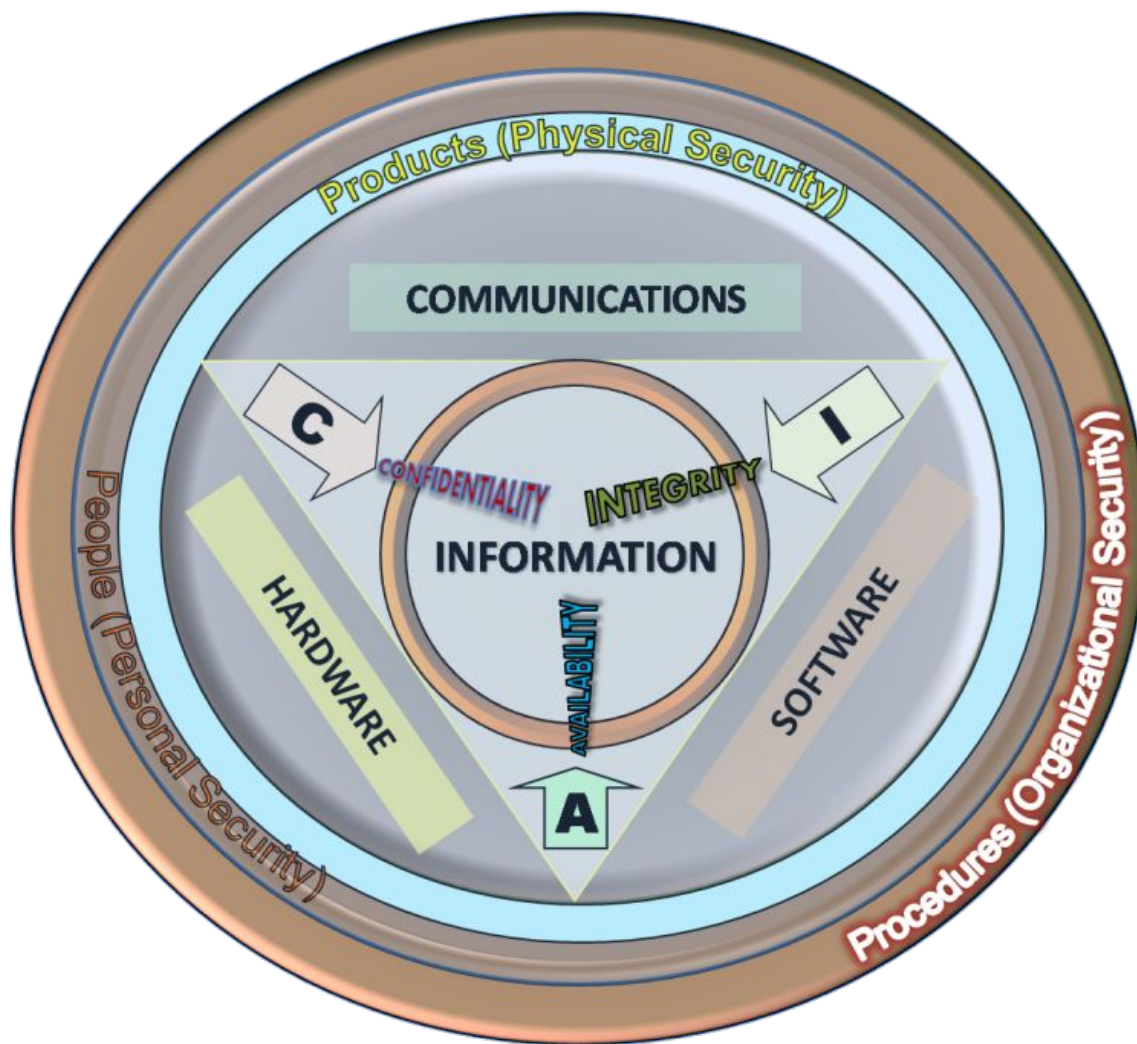
- Свойство информации, свидетельствующее о том, что информация не сделана доступной или не разглашена неуполномоченным лицам, организациям или процессам.

Аутентичность и достоверность



- **Аутентичность или подлинность** — свойство, гарантирующее, что субъект или ресурс идентичны заявленным.
- **Достоверность** — свойство соответствия предусмотренному поведению или результату;

Безопасность информации



Виды угроз

- Угрозы конфиденциальности.
- Угрозы доступности:
техногенные, непреднамеренные ошибки, пользовательская сложность ИС, инсайдеры.
- Угрозы целостности:
фальсификация данных (в т.ч. инсайдеры), нарушение атомарности транзакций.
- Угрозы раскрытия параметров защищенной компьютерной системы: новые угрозы, уязвимости, увеличение рисков.

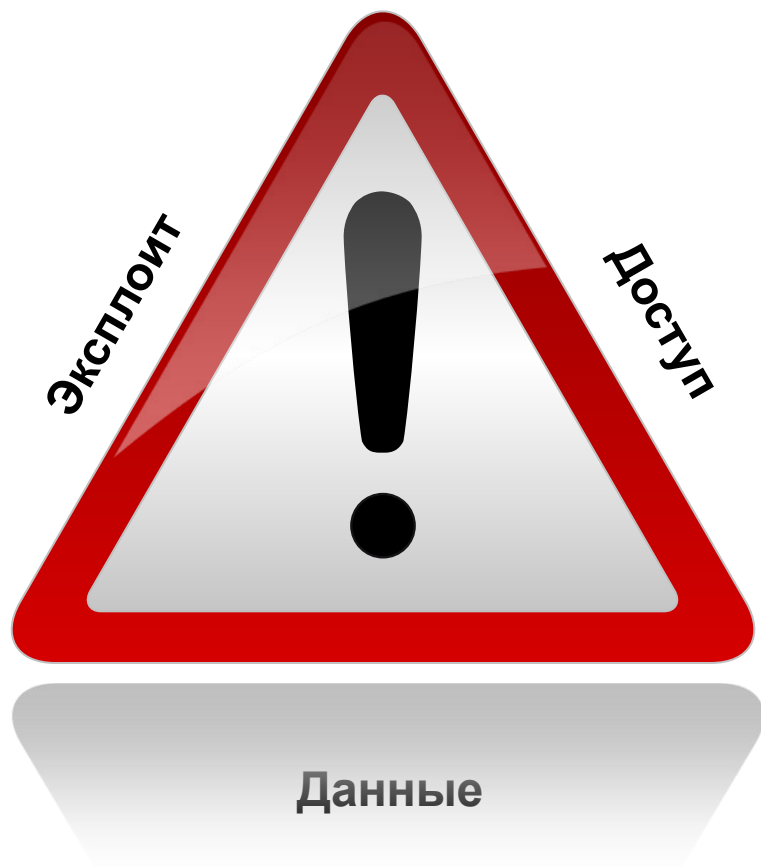


Источники угроз

- Внешние атаки.
- Инсайдерские атаки.
- Непреднамеренные ошибки.
- Отказ инфраструктуры.
- Внутренний отказ ИС.
- Юридические проблемы.
- Преднамеренные атаки физического уровня.



Треугольник безопасности 2009 ГОД



- Данные – цель и основной драйвер
- Эксплоит – уязвимость и механизмы ее использования
- Доступ – наличие принципиальной возможности доступа к системе

Треугольник безопасности 2011

ГОД



- Ресурсы – основная цель и инструмент.
- Инструменты – методы и средства преодоления защиты.
- Доступность – наличие принципиальной возможности доступа к системе.

Ресурс, как объект защиты

- Ресурсы:
 - Денежные средства пользователя
 - Процессорное время системы
 - Дисковое пространство
 - Пропускная способность канала подключения к сетям общего пользования
 - Информационные ресурсы



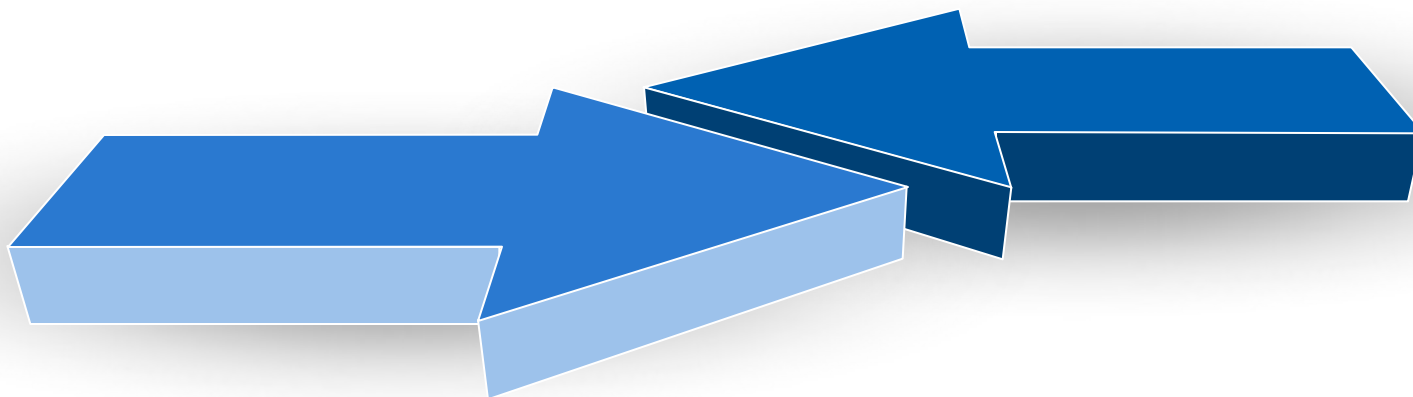
Проблема установления рационального баланса

Безопасность

- Затраты на безопасность
- Внедрение новых элементов СЗИ
- Управление жизненным циклом ИС
- Разграничение доступа

Эффективность

- Увеличение прибыли
- Сокращение расходов
- Накопление знаний
- Повышение осведомленности



«Голая» статистика

- 1995 год: 400 попыток проникновения в сеть ЦБ. Было похищено 250 млрд. рублей (TASS, Associated press, 09.1996).
- 1996 год: по статистике ФБР ущерб от компьютерных преступлений в США составил 136 млн. \$.
- 1998 год: 882 млн. \$.
- 2009 год: 100 млрд. \$.
- В России в 2003 году возбуждено 7423 уголовных дела в области компьютерных преступлений. В 2004 году – уже 13854 дела.
(по данным главного информационного центра МВД России)

«Голая» статистика

- Средний ущерб: от одного ограбления банка – 3400\$.; от одного мошеннического преступления – 24000\$.; от одной компьютерной кражи – 500 000 \$.
(по данным ФБР США)

Выводы:

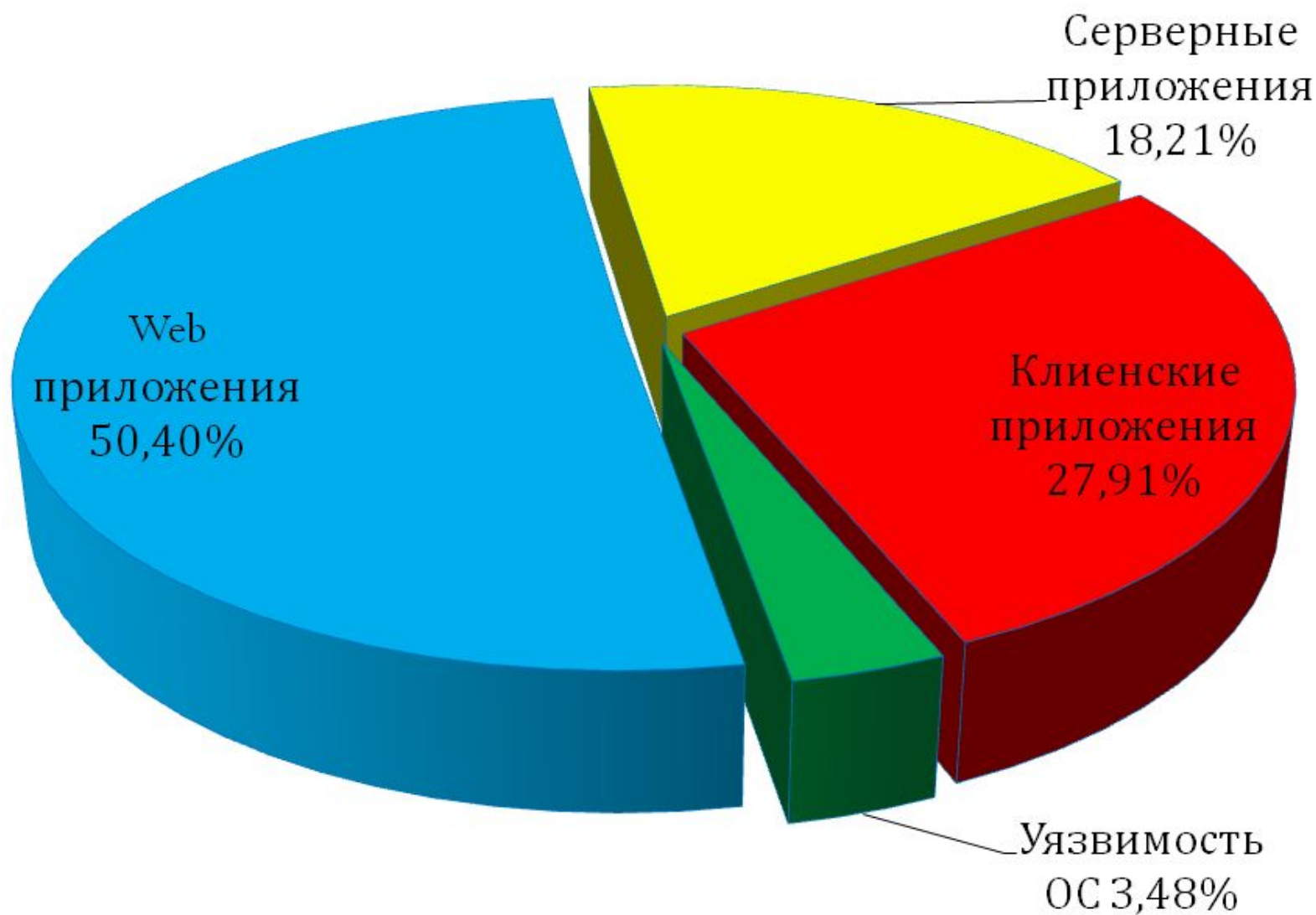
- Ежегодно ущерб от компьютерных преступлений возрастает в 2-2.5 раза.
- Фактическая сложность преступлений не растёт.
- С усложнением ИТ-инфраструктуры растут риски.
- С увеличением внедрения ИТ риски растут.

Реальное состояние защищённости

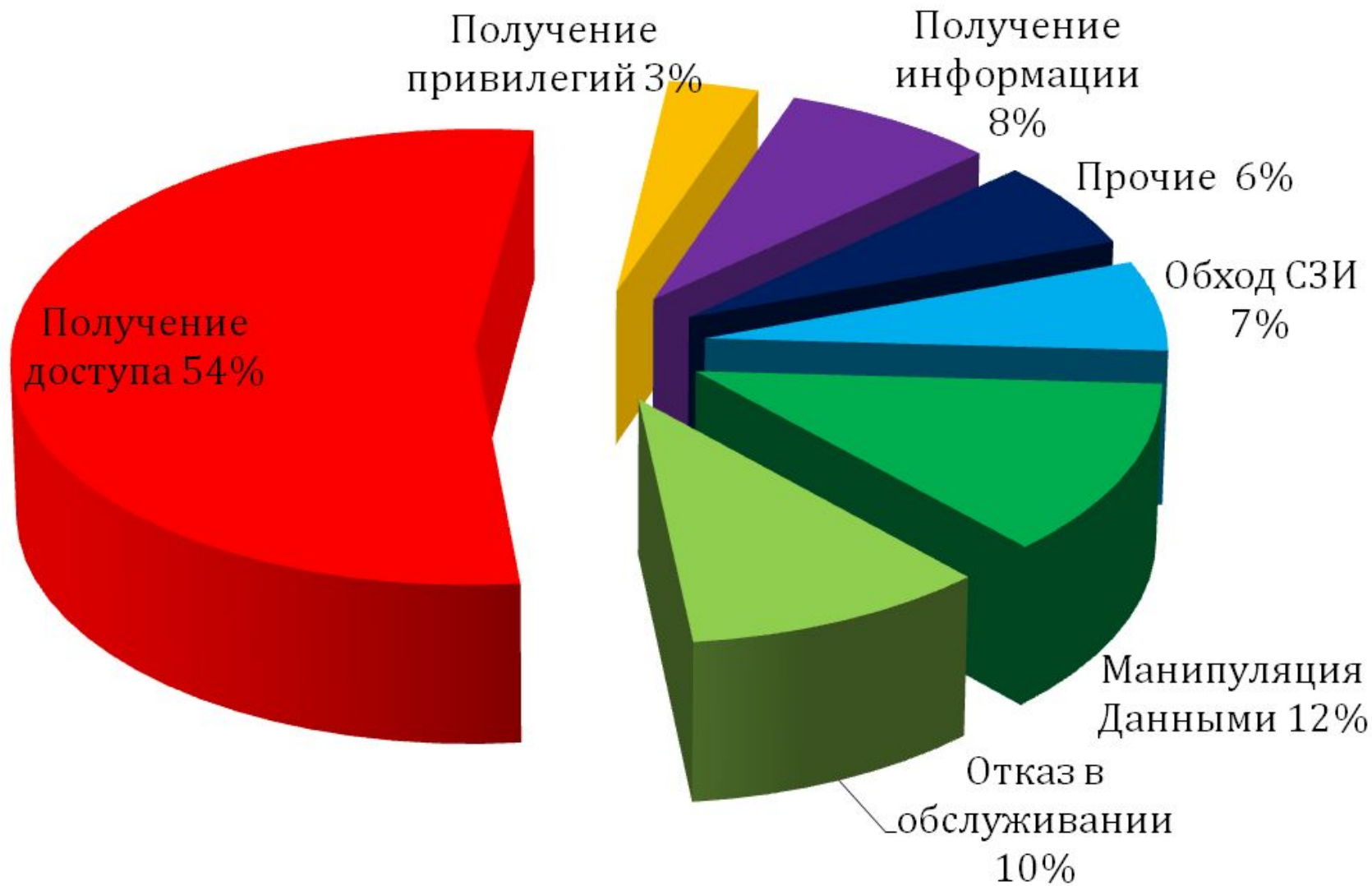
Результаты исследования Positive technologies по пентестам за 2012 год:

- 32% внешних нарушителей могут получить полный доступ ко внутренней сети компании.
- Внутренний нарушитель без привилегированных прав в 84% случаев может получить максимальные права в критически важных системах.
- 20% пользователей переходили по мошенническим ссылкам и вводили свои учетные данные / запускали заражённые файлы.

Обнаруженные уязвимости в 2011 году



Типы уязвимостей



Спасибо за внимание!