Аутсорсинг в области Информационной Безопасности

NextHop
Security

Типовые угрозы ИБ и их источники

Типовые угрозы безопасности

Вирусы и трояны–вредоносное ПО, которое распространяется в виде исполняемого кода через широко распространенные протоколы HTTP, FTP, SMTP и другие и заражает файлы на компьютерах

Черви–это вредоносное ПО, распространяемое по сети и проникающее на компьютеры через уязвимости в приложениях и ОС

Фишинг–это метод, в рамках которого пользователи кликают по ссылкам и попадают на сфальсифицированные сайты, разработанные для кражи персональных данных

Фарминг–это метод перенаправления легитимного запроса на подставной сайт с целью кражи персональных данных

Шпионское ПО–это ПО, которое мониторит действия и поведение пользователей (нажатия клавиш, пароли, посещаемые сайты и т.д.) и передает эту информацию злоумышленникам

Отказ в обслуживании–атака, приводящая к нарушению работоспособности Интернет-или Интранет-ресурсов

Источники угроз

Уязвимости приложений позволяют злоумышленникам получить доступ к базам данных или повысить уровень своих привилегий на доступ к приложениям

Некорректный доступ к данным через некорректно настроенные или устаревшие защитные механизмы

Уязвимости ОС позволяют злоумышленникам контролировать компьютеры, красть информацию и получать несанкционированный доступ к системе

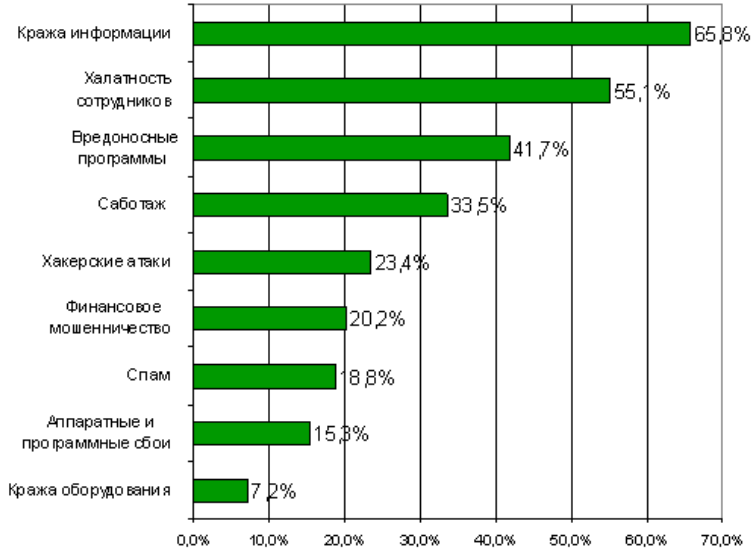
Сообщения электронной почты могут содержать подмененные ссылки (фишинг) и вложения, инфицированные шпионским ПО, вирусами и другими типами вредоносного ПО

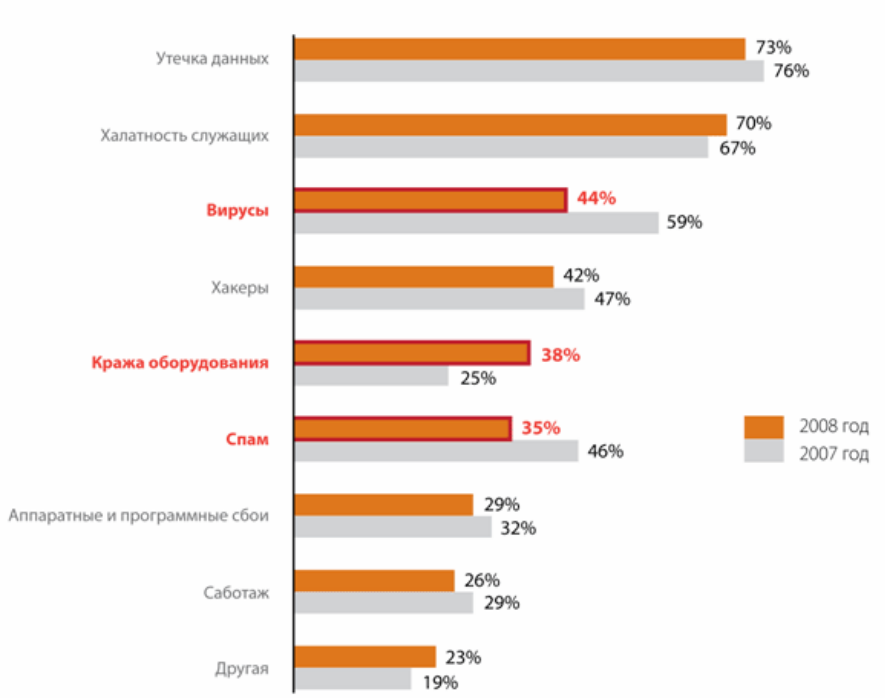
Использование Интернет включает загрузку нелицензионного и вредоносного ПО, посещение ненужных сайтов и т.д.

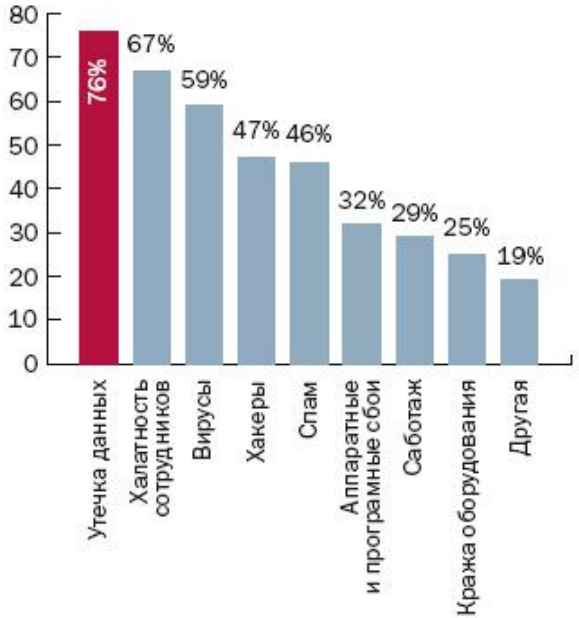
Доступ пользователей к информации и ресурсам, которые не требуются для выполнения служебных обязанностей

NextHop
Security

Статистика по реализации угроз ИБ







NextHop Security

Динамика направления ИБ

Как мы видим – **главная угроза** на сегодня, это утечка данных, представляющих коммерческую или производственную ценность, а **главный «инструмент»** утечки – халатные или заинтересованные в данной информации сотрудники

Существует масса **коробочных решений**, которые отлично документированы и поставляются с бесплатной, ограниченной лишь временем, поддержкой – но, сразу же появляется **человеческий фактор** и варианты инсайдерства

NextHop
Security

Аутсорсинг ИБ – плюсы и минусы

Основные преимущества

- значительно дешевле постоянного найма требуемых специалистов
- отсутствует человеческий фактор «знакомства» сотрудников
- нет конкретной заинтересованности специалиста в какой-либо информации, так как он с трудом представляет её ценность и доступ его к файлам полностью ограничивается применяемым решением ИБ
- возможность удалённого реагирования на инциденты в любое время суток
- консультирование по вопросам всего спектра ИБ, возможность привлечения экспертов требуемого уровня без дополнительных затрат
- плановая подготовка ваших сотрудников до необходимого уровня знаний
- возможности независимых аудитов по заданным направлениям

NextHop Security

Аутсорсинг ИБ – плюсы и минусы

Некоторые недостатки и способы решения

- отсутствие взаимопонимания между специалистами - «втыкание палок в колёса», перевод претензий в адрес друг друга, вместо поиска конструктивного решения (решается на уровне руководства – административным документом)
- возможность несогласованного заранее доступа к оборудованию заказчика (решается установкой подходящей системы мониторинга и настройкой прозрачной для ответственных специалистов политики)
- некоторая латентность в выполнении пожеланий заказчика на системах ИБ (два варианта решения – обучение сотрудников, либо изменения плана подписки с чётко заданным интервалом реакции на тот или иной запрос)
- предрассудки – поиск решения в процессе ☺

NextHop
Security

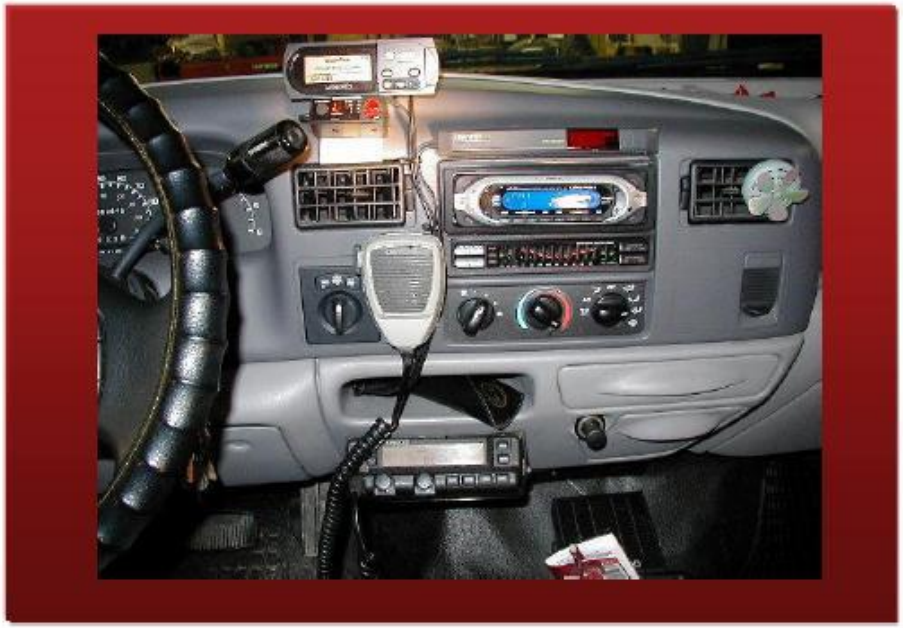
Надёжные системы ИБ

NextHop Security

Преимущества “collaboration” в ИБ

NextHop
Security

Преимущества комплексного подхода



Меньше сложности, больше удобства

Лучшее взаимодействие, рост эффективности

Меньше устройств, снижение CapEx и OpEx

NextHop
Security

О стандартах и законодательстве

Законодательство

Соответствие законодательным требованиям к системам защиты автоматизированных систем позволяет защититься от недобросовестной конкуренции и внимания проверяющих организаций.

- №98-ФЗ «О коммерческой тайне»
- №152-ФЗ «О персональных данных»
- №5485-1-ФЗ «О государственной тайне»
- СТО БР (Стандарт Банка России)

Стандарты

ISO 9001,

ISO 27001,

ISO 17799,

ISO 13569,

ISO 18044,

BS 25999,

СТР-К, РД

NextHop
Security

Вендоры по продуктам ИБ

S-terra CSP (VPN Gate) – сертифицированные ФСБ России СКЗИ

F5 Networks (BIG-IP ASM) – МЭ уровня приложений

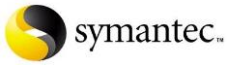
Verano (Industrial Defender) – средства защиты систем промышленной автоматизации

Cisco Systems/netForensics (CiscoWorks SIMS, MARS) – управление событиями ИБ

Embarcadero (DSAuditor) – аудит доступа к БД

IronPort Systems (IronPort) – защита от «спама»

Microsoft (Windows, MS SQL, ISA) – сертифицированные ФСТЭК России ОС, СУБД, МЭ



Аутсорсинг в области
Информационной Безопасности

ВОПРОСЫ?

Контакты:

+7 985 9994824 Пётр Кузеев
+7 916 6411027 Вячеслав Семёнов

Удачи в делах!

NextHop
Security