Доклад

Возможно ли обеспечить 100% гарантию безопасности организации

Пшиченко
Дмитрий Викторович
Эксперт секции "Информационная безопасность ТЭК" консультативного Совета при председателе Комитет Государственной Думы Федерального Собрания РФ по энергетике

Москва 2015

Примеры угроз информационной безопасности организации

Направления обеспечения безопасности	Техногенные		Природные
	Преднамеренные	Случайные	
Контроль физического доступа	Бомбардировка	Сон вахтерши	Торнадо
Сохранность оборудования	Вандализм	Запыление	Шаровые молнии
Управление коммуникациями	Прослушивание сети	Флуктуации в сети	Магнитные бури
Защита информационных хранилищ	Взлом парольной системы	Сбой криптосредств	Грибки
Управление непрерывностью деятельности	Последствие DOS-атаки	Последствия тестов на проникновения	Карстовые процессы
Соответствие законодательству	Компьютерное пиратство	Тиражирование персональных данных	Природные пожары

От обеспечения безопасности к управлению киберрисками

Киберпространство – это сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, ПО, интернет сервисов посредством технологических устройств и сетевых связей.

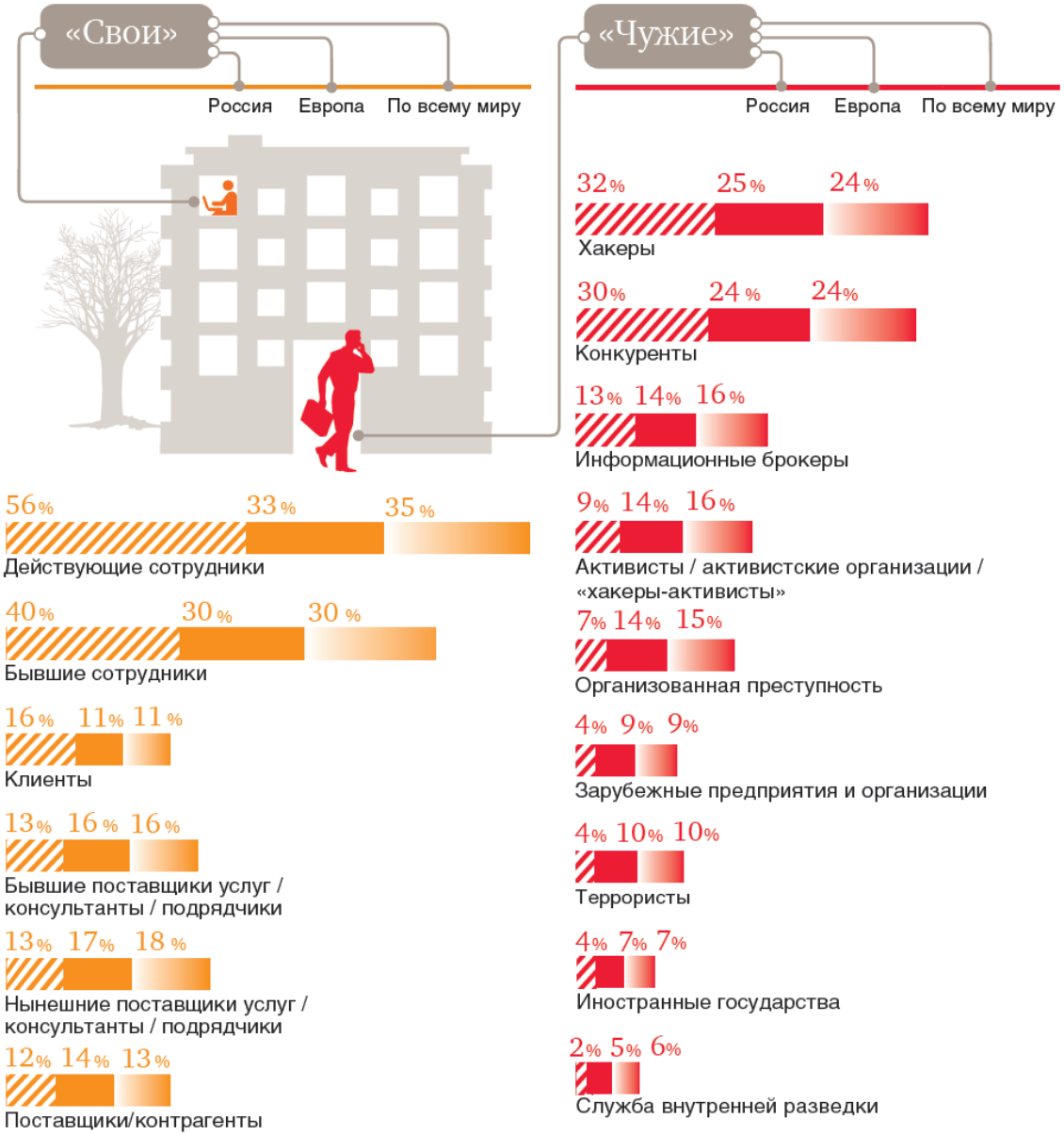
Кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

Виновники инцидентов информационной безопасности, 2013–2014 гг. * «Свои» или «чужие»

Сотрудники компании — не единственный источник растущей угрозы со стороны «инсайдеров».
В 2014 году процентная доля инцидентов информационной безопасности, связанных с действиями нынешних и бывших поставщиков услуг, консультантов и подрядчиков, увеличилась соответственно до 18% и 15%.

Преступления, связанные с действиями «инсайдеров», дороже обходятся компании по сравнению с инцидентами, в которых виновны «чужие». Тем не менее во многих компаниях до сих пор не внедрена программа противодействия угрозам со стороны «инсайдеров», и, соответственно, такие компании не готовы предотвращать и выявлять внутренние угрозы, а также должным образом на них реагировать.

* Глобальное исследование по вопросам обеспечения информационной безопасности за 2015 год (The Global State of Information Security®Survey 2015), проведенное фирмой PwC и журналами CIO и CSO.



Оценка потерь от внутренних угроз

Ключевыми рисками внутри компаний являются :

- уязвимости в ПО (48%),
- незнание сотрудниками правил IT-безопасности, приводящее к случайным утечкам данных (36%),
- намеренное раскрытие конфиденциальной информации сотрудниками (23%).

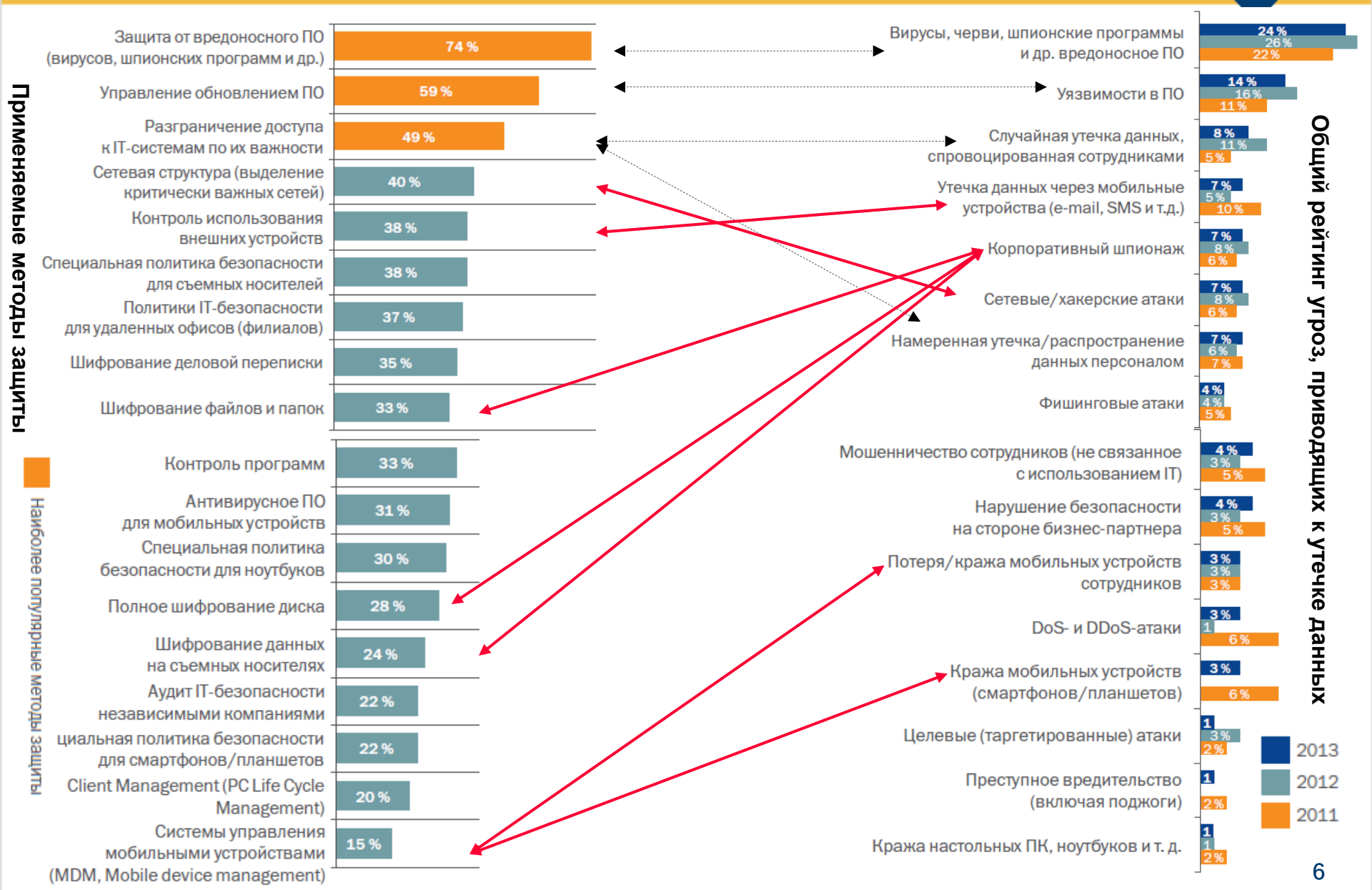
Информационная безопасность бизнеса, 2014. Исследование лаборатории Касперского.

Применяемые методы защиты

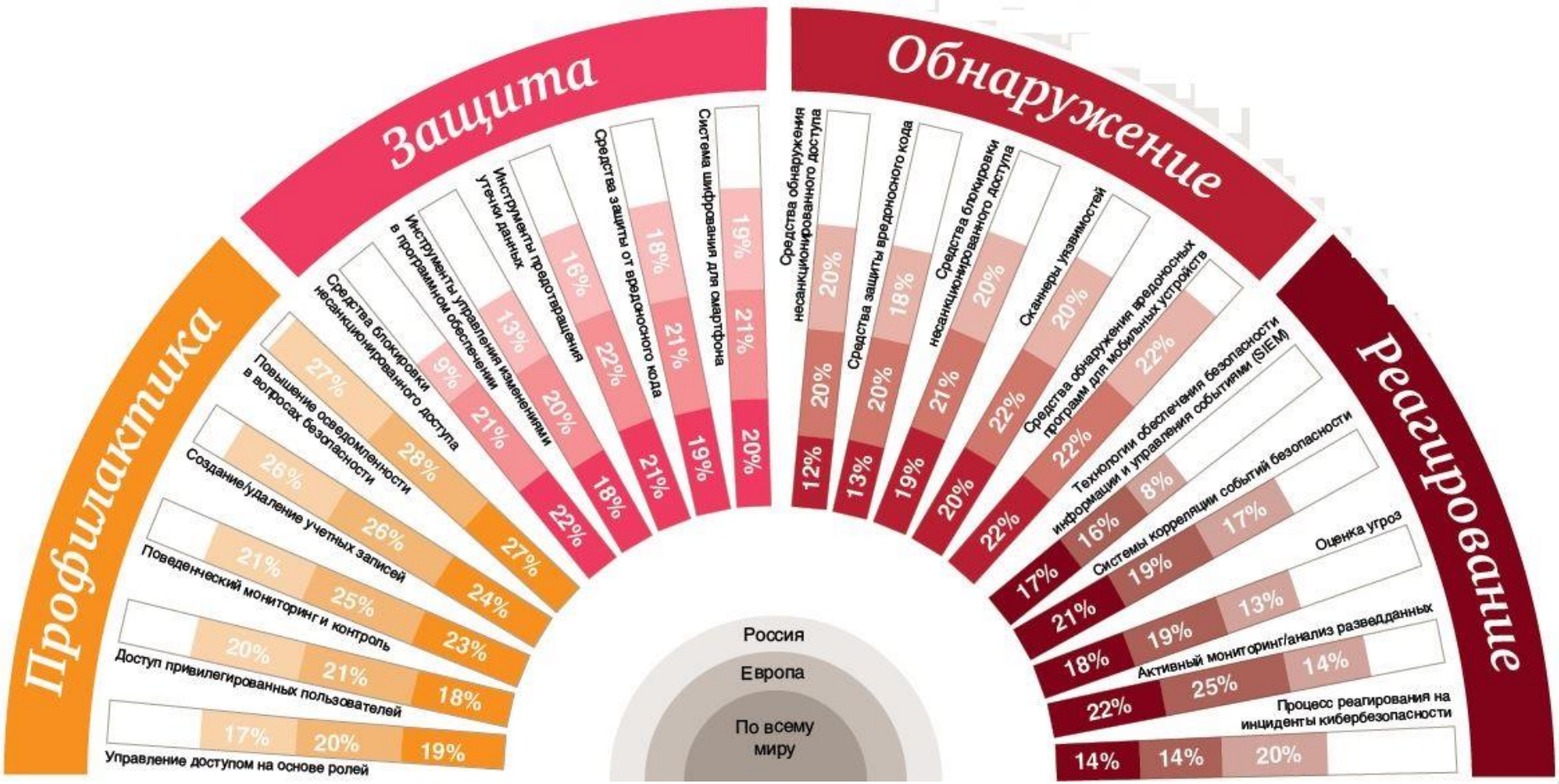
Большинство компаний рассматривают антивирусное ПО как основное средство для обеспечения информационной безопасности, а компании, признающие необходимость использования дополнительных средств, таких как MDM-системы или средства защиты от утечек и перехвата критически важной бизнес-информации, пока в меньшинстве. Эта тенденция сохраняется уже много лет, в то время как ландшафт киберугроз постоянно меняется.

Информационная безопасность бизнеса, 2014. Исследование лаборатории Касперского.

Применяемые методы защиты в сравнении с угрозами, приводящих к утечкам данным



Инвестиции в процессы и технологии, обеспечивающие предупреждение и выявление рисков информационной безопасности.



* Глобальное исследование по вопросам обеспечения информационной безопасности за 2015 год (The Global State of Information Security®Survey 2015), проведенное фирмой PwC и журналами CIO и CSO.

ПРИЛОЖЕНИЯ

Национальные стандарты в области информационной безопасности

Обозначение ГОСТ	Наименование
Системы менеджмента информационной безопасности	
ГОСТ Р ИСО/МЭК 27000-2012	ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
ГОСТ Р ИСО/МЭК 27001-2006	ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
ГОСТ Р ИСО/МЭК 27002-2012	ИТ. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
ГОСТ Р ИСО/МЭК 27003-2012	ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности
Управление рисками	
ГОСТ Р ИСО/МЭК 27005-2010	ИТ. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
Оценка безопасности	
ГОСТ Р ИСО/МЭК 15408-2012	ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий
ГОСТ Р ИСО/МЭК 18045-2013	ИТ. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий
ГОСТ Р ИСО/МЭК ТО 19791-2008	ИТ. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем
Гарантии безопасности	
ГОСТ Р ИСО/МЭК 15026-2002	ИТ. Уровни целостности систем и программных средств
Сетевая безопасность	
ГОСТ Р ИСО/МЭК 27033-1-2011	ИТ. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции
Безопасность приложений	
проект ГОСТ Р (согласно планам ТК 362)	Требования по обеспечению безопасности разработки программного обеспечения
Обеспечение непрерывности бизнеса	
ГОСТ Р ИСО/МЭК 27031-2012	ИТ. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса
ГОСТ Р ИСО/МЭК ТО 18044-2007	ИТ. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
ГОСТ Р 53647.4-2011	Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности
Проектирование систем безопасности	
ГОСТ Р ИСО/МЭК 21827-2010	ИТ. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса

Положения стандарта ISO 27032 опираются на организационно-технические меры, определенные, главным образом, в стандартах 27000-серии, ссылаются на подходы к оценке безопасности продукции и систем по линии «Общих критериев», а также ссылаются на рекомендации ITU (Международный союз электросвязи).

В РФ сложилась представительная нормативная база информационной безопасности, которая может быть полезна при решении задач кибербезопасности.

Приведены примеры национальных стандартов, гармонизированных с ISO 27032.

СПАСИБО
ЗА ВНИМАНИЕ!

ФЕДЕРАЛЬНОЕ СОБРАНИЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ГОСУДАРСТВЕННАЯ ДУМА

ПШИЧЕНКО
Дмитрий Викторович

Эксперт секции "Информационная безопасность ТЭК"
консультативного Совета при председателе
Комитет Государственной Думы
Федерального Собрания РФ по энергетике

E-mail: dmitry@pshychenko.com

Тел.: 8 (495) 969-08-04
Моб.: +7-916-669-62-99