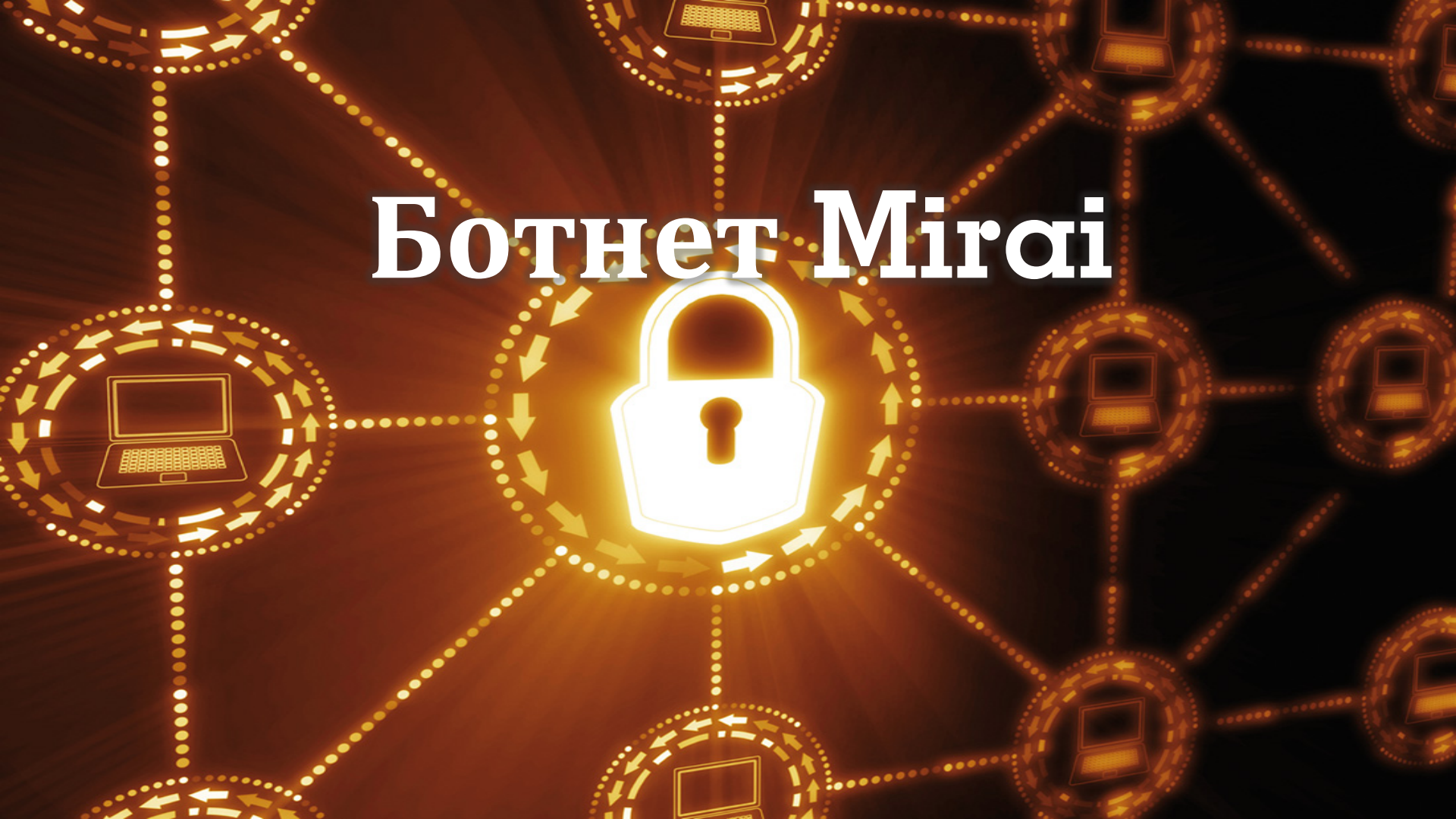


**Кибербезопасность
это
ВАЖНО**



Ботнет Mirai



Ботнет Mirai

Использует IoT устройства, такие как IP камеры, DVR, роутеры и т.д. для запуска крупных DDoS атак на различные интернет сервисы

Рекордные атаки с ботнет Mirai достигали 1 Тбит/с

Сентябрь 2016 - KrebsOnSecurity.com

Октябрь 2016 - Dyn.com

Многие интернет сервисы, в т.ч. такие как Amazon, PayPal не были доступны или столкнулись с серьезными проблемами

Что такое
BotNet?



roBot & Network





DDoS

Distributed Denial of Service

распределенный отказ в
обслуживании

Как можно
заразиться?



user	pass	user	pass	user	pass
666666	666666	root	7ujMko0admi	guest	12345
888888	888888	root	7ujMko0vizx	guest	guest
admin	(none)	root	888888	mother	fucker
admin	1111	root	admin	root	(none)
admin	1111111	root	anko	root	0
admin	1234	root	default	root	1111
admin	12345	root	dreambox	root	1234
admin	123456	root	hi3518	root	12345
admin	54321	root	ikwb	root	123456
admin	7ujMko0admin	root	juantech	root	54321
admin	admin	root	jvbsd	root	666666
admin	admin1234	root	klv123	root	vizxv
admin	meinsm	root	klv1234	root	xc3511
admin	pass	root	pass	root	xmhdipc
admin	password	root	password	root	zlxx.
admin	smcadmin	root	realtek	root	Zte521
admin1	password	root	root	service	service
administrator	1234	root	system	supervisor	supervisor
Administrator	admin	root	user	support	support
user	user	ubnt	ubnt	tech	tech

«Вшитые»

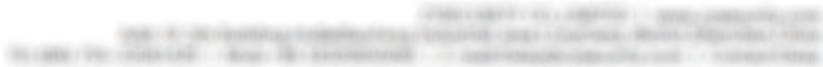
ЛОГИН

и пароль

```
mirror_mod = modifier_ob.  
#set mirror object to mirror  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
  
#selection at the end -add  
mirror_ob.select= 1  
mirror_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier_ob.  
mirror_ob.select = 0  
= bpy.context.selected_object  
data.objects[one.name].select  
print("please select exactly  
  
-- OPERATOR CLASSES ----  
  
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
error X"  
  
context):  
context.active_object is not
```

Черный ход
в прошивке
камеры





UNIQUE SYSTEM - SUPER PASSWORD - FOR DVR NVR IPC

2017 January	
1	y6rEnN9136
2	NEWdMf773
3	nAwk4f4792
4	HcB4Qs1199
5	hdiQJ80
6	lrI0bG1201
7	FKLw0j4808
8	nGtzCB827
9	eEo3T59264
10	Q0WbaW9136
11	XgQ6xi773
12	4gv8me4792
13	lluKNB1199
14	xePFvG0
15	9EhuEg1201
16	8UTjLw4808
17	Q1rm80827
18	tUjlJc9264
19	KCHQN6125
20	l4iuaN773
21	A32uf4792
22	QGT2Va1199
23	zaRezi0
24	fi5aiA1201
25	vM04Aj4808
26	cCeimV827
27	94Fvpm9264
28	7d1gdX125
29	yOAE1g3416
30	xHlmlMv4792
31	ChxUY61199

2017 February	
1	hGz3p9773
2	fDyRFB4792
3	2DxRIK1199
4	lYJ59Q0
5	bDNPUL1201
6	GR6Y0e4808
7	7lJ6yy827
8	xn2uyV9264
9	u7uUQh125
10	UA10mr773
11	Snqh6u4792
12	KJZQJ1199
13	aF01u0
14	0
15	ao1sy14808
16	JlOdAl827
17	ijyw6A9264
18	KFQ9jX125
19	L9ZAuy3416
20	Yz8KUc4792
21	cTRiX81199
22	4Cjmnz0
23	VqlQwB1201
24	chlqGR4808
25	0qPXm827
26	hCmUHZ9264
27	uldSCW125
28	50d44eg3416

	2017 March
1	IVKN5o4792
2	OC0Z9L1199
3	AuKUG00
4	g28cFK1201
5	zbkby5A808
6	OJkvHG827
7	zgmlOO9264
8	f7m2mH125
9	yUxLs3416
10	IAH5ge4792
11	Lr1zBn1199
12	yGBVQ0
13	hUNJPk1201
14	hWNVN1201
15	qR0R01201
16	2hyMU39264
17	jNBAL125
18	u87vdt3416
19	OUPVab9143
20	Dq62je1199
21	bO5KeD0
22	oWBhp11201
23	29ksvt4808
24	n9GTa827
25	76f7899264
26	BrSTOu125
27	pJEObk3416
28	QaBbvR9143
29	8dyncx7312
30	SLEOW00

	2017 April
1	Q5yeRg1199
2	zq9Ty0
3	9Quiam1201
4	SgtyKo4808
5	B8rc1u827
6	zla2ot9264
7	hgJ9hA125
8	5u291A3416
9	jTDUSC9143
10	xbvwZo1199
11	R7SzrG
12	7oQTzk1201
13	MUule34808
14	gUu9p264
15	ShaEt1125
16	V5O2Y3416
17	ZhnW029143
18	gWQZRu7312
19	Kw47Bw0
20	CISW201201
21	jsafKF4808
22	pw5Z6R827
23	EN2RCM9264
24	fNwKkQ125
25	hpJY7w3416
26	Gtokf59143
27	UB6cj67312
28	3XK8ta7929
29	akeK7o1201

2017 May	
1	sEYrY00
2	Cn4R3Y1201
3	VCAg4G4808
4	ogVNV0827
5	fXCIL49264
6	HxjJEv125
7	z3W1cr3416
8	5Qdqja9143
9	461WuM7312
10	YJT6N0
11	SekbAI1201
12	pmieOL4808
13	sloanv827
14	461WuM7312
15	461WuM7312
16	6ot6RO3416
17	LmkVnJ9143
18	VJH2sG7312
19	B5u2JZ7929
20	Fu55LG1201
21	vUrT844808
22	FWQ9Kg827
23	T6TWm49264
24	RYPxrKI25
25	CChAeB3416
26	FbeNe29143
27	nLIDM97312
28	ftdcXw7929
29	z229dk1000
30	Cim7HR4808
31	PaQboh827

2017 June	
1	s6udvo1201
2	L7MbXd4808
3	3bvZze827
4	7Lhs4l9264
5	k6MTRC125
6	8aWgfy3416
7	G88v639143
8	gC1L7c7312
9	W4DDYM7929
10	t5hkC31201
11	tMwcc54808
12	XiFgk827
13	FyPzK9264
14	u8U125
15	nv38sg3416
16	G9vOqh9143
17	pleWQA7312
18	j2xFCT929
19	Guo3ui1000
20	jluOx54808
21	xfIkDe827
22	c8dmJm9264
23	wwWlrr125
24	1kyPYVY3416
25	R5cwEB9143
26	WeD3c7312
27	A3gTgZ929
28	xUeLpS1000
29	6hoW5n6531
30	Bx5qPR827

Fast delivery, good quality, best price

Какие еще угрозы?



Смена паролей на устройствах видеонаблюдения

Сброс на заводские настройки

Странные надписи в оверлее

**Кого-то уже
коснулось**



**Каковы были
убытки**



Атака хакеров на сеть
видеонаблюдения г.
Вашингтон. 70% серверов не
работали 12-15 января



Кибербезопасность глазами Axis

Партнеры в безопасности

Партнеры в безопасности

**Активное участие
всех поставщиков и
пользователей
системы**

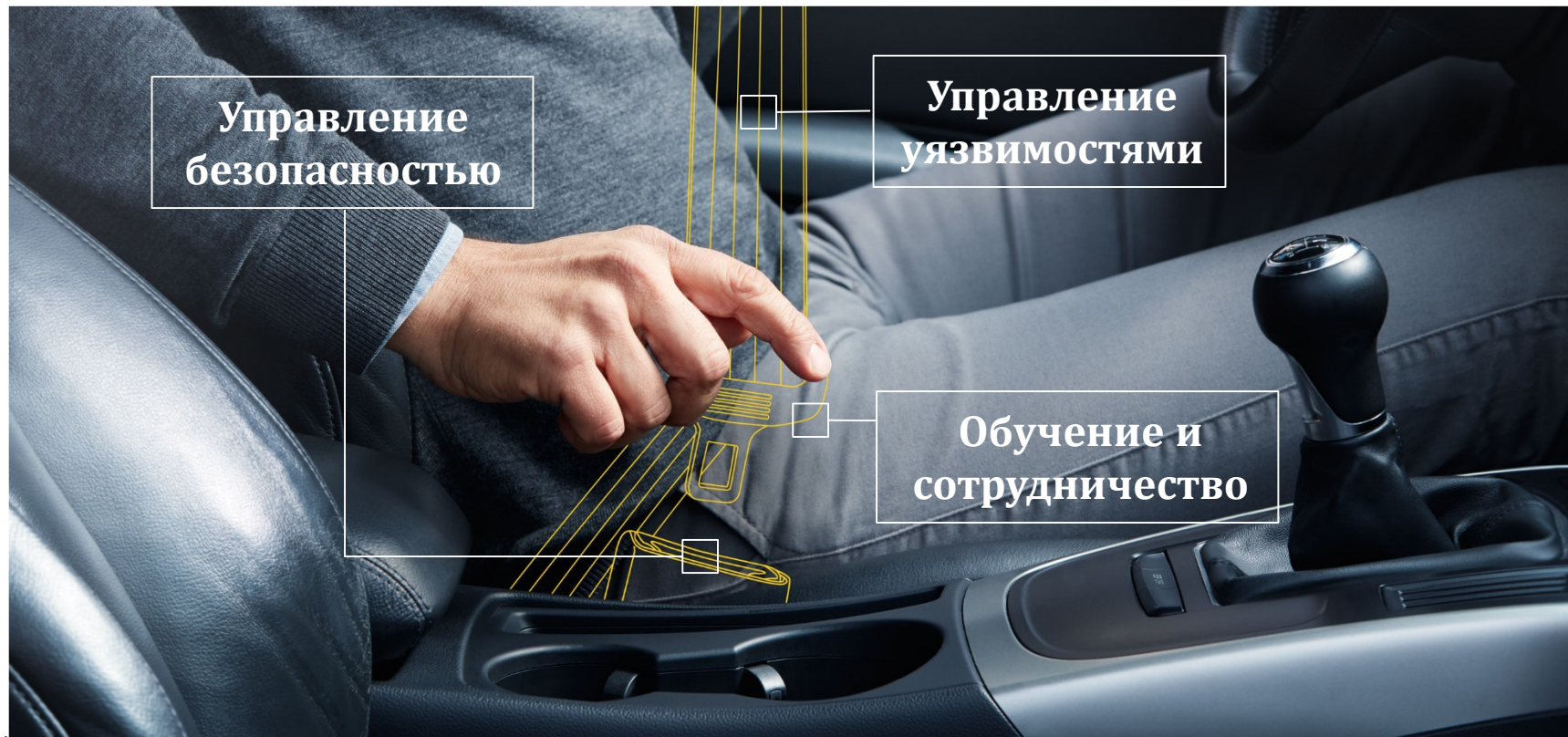


Управление рисками и их минимизация

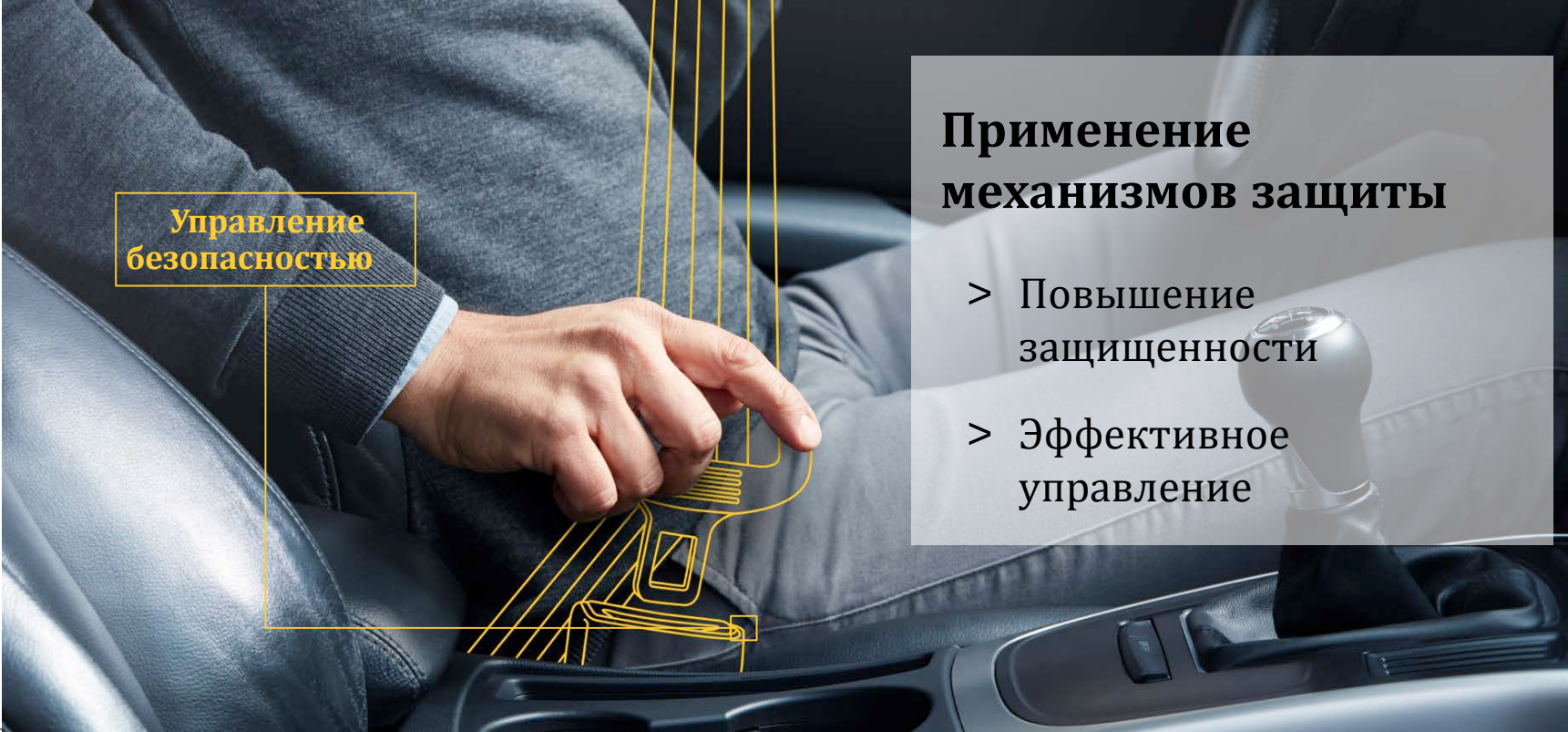
- > Риск = вероятность * воздействие
- > Понимание угроз и воздействия



Три уровня защиты



Управление безопасностью



Управление
безопасностью

Применение механизмов защиты

- > Повышение защищенности
- > Эффективное управление

Лучший друг – руководство по усилению защиты



1. Introduction	3
1.1 Security cameras in a network environment	3
1.2 Limit Internet exposure	3
1.3 Limit local network exposure	3
2. About the protection levels	4
3. Default protection	4
4. Standard protection	5
4.1 Factory default settings	5
4.2 Use latest firmware	5
4.3 Set master password	5
4.4 Create a video client account	5
4.5 Configure network settings	6
4.6 Set time and date	6
4.7 Disable audio	6
4.8 Edge Storage Encryption	6
5. Enterprise protection	7
5.1 Open ports	7
5.2 HTTP digest authentication	7
5.3 Domain and host name	7
5.4 Disable unused services	8
5.4.1 FTP server	8
5.4.2 SSH – Secure Shell	8
5.4.3 ARP/Ping setting of IP address	8
5.4.4 AXIS Device Dispatcher – AVHS	8
5.4.5 Network discovery protocols	9
5.4.6 SOCKS	9
5.4.7 Always multicast video	9
5.4.8 QoS – Quality Of Service	9
5.5 IP address filter (IP tables)	9
5.6 HTTPS Encryption	10
6. Managed enterprise protection	10
6.1 IEEE 802.1X network access control	10
6.2 SNMP monitoring	10
6.3 Remote System Log	11
About this document	12
Contact information	13
Support	13

Набор конкретных шагов по повышению защищенности



AXIS Camera Management

- Прошивка
- Пароли
- IP адреса
- АСАР приложения
- Управление сертификатами

New firmware versions exists for 5 devices									
61 devices, 1 selected									
MAC Address	Status	Address	Host Name	Model	IEEE 802.1X	Firmware	DHCP	Server	
00408C10003F	OK	172.25.64.178		AXIS Q3615	Missing client certificate	15+snapshot...	Yes	LAPOLALN	
00408C100153	OK	172.25.71.10		AXIS M3106-L	Missing client certificate	6.15.4	Yes	LAPOLALN	
00408C184618	OK			AXIS Q8685-E	Missing client certificate	16+snapshot...	Yes	LAPOLALN	
00408C184A4E	OK	172.25.64.179		AXIS P3384-V	Missing client certificate	5.60.1.4	Yes	LAPOLALN	
00408C185C81	Certificate expired	172.25.77.105		AXIS Q6000-E	Missing client certificate	5.65beta15	Yes	LAPOLALN	
00408C185E21	OK	172.25.71.10		AXIS P5635-E	Missing client certificate	6.20beta5	Yes	LAPOLALN	
00408C185F3C	OK	172.25.68.24		AXIS Q3615	Missing client certificate	6.15.3	Yes	LAPOLALN	
00408C185F3D	Not accessible	172.25.66.9		AXIS Q3617	Missing client certificate	15+snapshot...	Yes	LAPOLALN	
00408C186048	Not accessible	172.25.72.116		AXIS Q1775	Missing client certificate	17+snapshot...	Yes	LAPOLALN	
00408C186AD3	OK	172.25.71.10		AXIS C1004-E	Missing client certificate	1.25.1	Yes	LAPOLALN	
00408C1868C5	OK	169.254.90.151		AXIS M3045-V	Missing client certificate	6.15.4.1	Yes	LAPOLALN	
00408C186E02	OK	172.25.71.79		AXIS Q6054-E	Missing client certificate	6.25.1.1	Yes	LAPOLALN	
00408C186E81	OK	172.25.71.10		AXIS Q1942-...	Missing client certificate	6.50.1	Yes	LAPOLALN	
00408C1870E2	OK	172.25.71.251		AXIS Q1942-...	Missing client certificate	16+snapshot...	Yes	LAPOLALN	
00408C1870E7	OK	172.25.72.78		AXIS Q1942-...	Missing client certificate	6.45_beta2	Yes	LAPOLALN	
00408C1870E8	OK	172.25.71.10		AXIS Q1941-...	Missing client certificate	16+snapshot...	Yes	LAPOLALN	
00408C1870EA	OK	172.25.71.10		AXIS Q1941-...	Missing client certificate	6.50.1.2	Yes	LAPOLALN	
00408C1872C1	OK	172.25.68.255		AXIS M2026-...	Missing client certificate	16+snapshot...	Yes	LAPOLALN	
00408C56382A	OK	172.25.71.242		AXIS Q3505...	Missing client certificate	15+snapshot...	Yes	LAPOLALN	
00408C92FD66	Not accessible	172.25.67.149		AXIS 215 PTZ	Unsupported firmware	4.49	Yes	LAPOLALN	
00408C94182D	OK	172.25.68.65		AXIS P3301	Missing client certificate	RestrictedAre...	Yes	LAPOLALN	
00408CA569D6	OK	172.25.69.248		AXIS P3343	Unsupported firmware	5.40.9	Yes	LAPOLALN	
00408CA5C29A	OK	172.25.72.140		AXIS Q1910	Missing client certificate	5.50.4.1	Yes	LAPOLALN	
00408CAD6999	OK	172.25.72.85		AXIS M1054	Unsupported firmware	5.40.9	Yes	LAPOLALN	
00408CB96108	OK	172.25.70.203	P3367-fredsv.ca...	AXIS P3367	Missing client certificate	16-16.39.0	Yes	LAPOLALN	

В будущих версиях прошивки

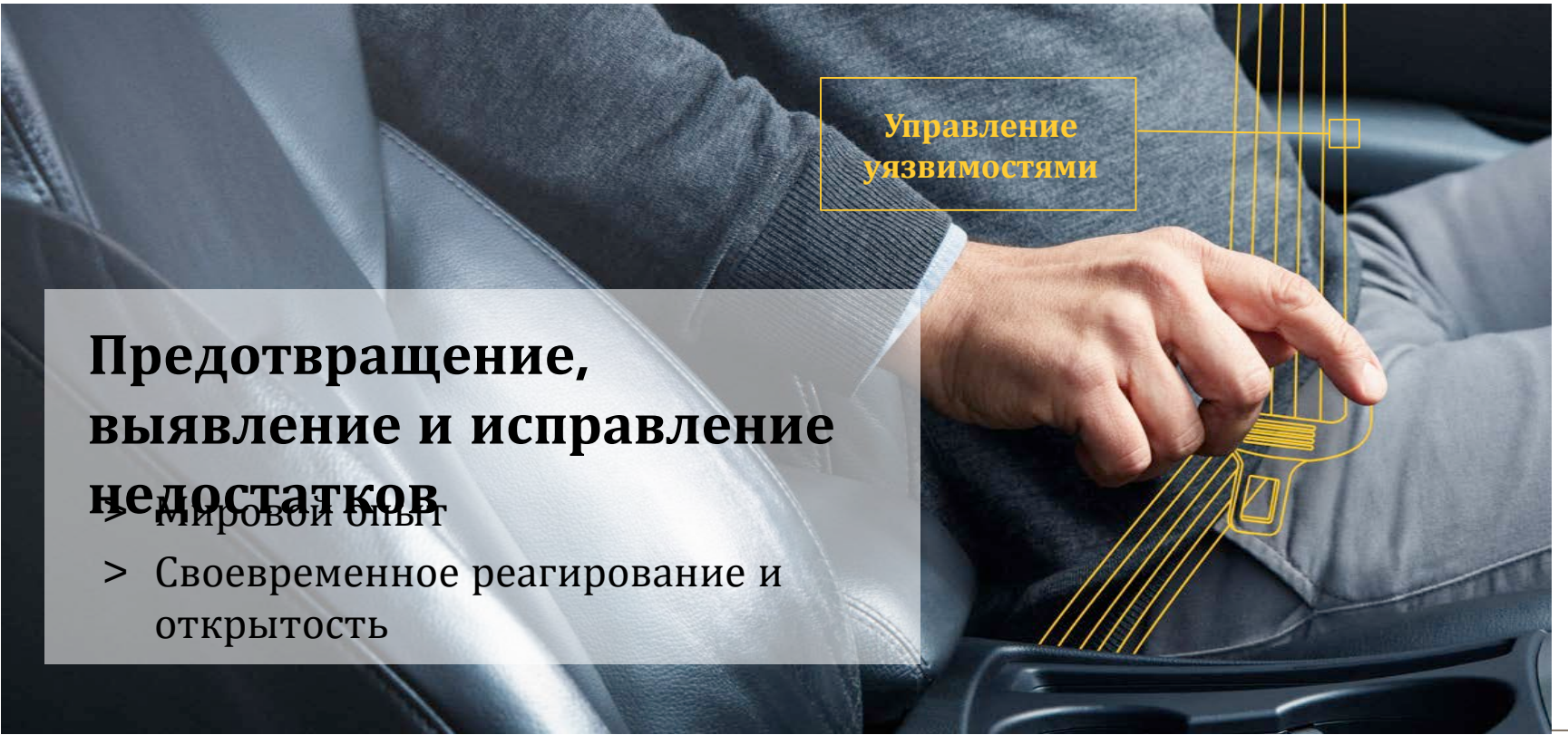
- Сложность пароля
 - Мин. 8 знаков
- Шифрование логина
- Предотвращение массовых попыток входа
- Отключение неиспользуемых служб
- Обнаружение подделок:
 - Прошивка
 - АСАР приложение

System Upgrade

The system is about to be upgraded.
Please wait.

Close

Управление уязвимостями



Управление
уязвимостями

**Предотвращение,
выявление и исправление
недостатков**

- > мировой опыт
- > Своевременное реагирование и открытость

Управление уязвимостями: когда что-то пойдет не так

COMMUNICATIONS

Lund, July 6, 2016

Axis recommends firmware upgrade to address security vulnerability

A critical security vulnerability has recently been discovered affecting products that are exposed to the Internet. Axis strongly recommends that customers upgrade to latest firmware releases.

A critical security vulnerability has been discovered in Axis products, with firmware versions between 5.20 to 6.20.X. At risk are products that are exposed to the Internet. If the products are exploited, the intruder has the potential to get control of the product.

Devices behind a protected network, network cameras connected to AVHS (AXIS Video Hosting System) and network cameras part of AXIS Companion solution are at low risk.

Обучение и сотрудничество



Обмен знаниями

- > Повышение осведомленности
- > Обмен опытом
- > Сотрудничество при создании решений

Обучение и
сотрудничество

Риски и рекомендации

Общие рекомендации

Общие рекомендации

- > Политика учетных записей
- > Политика паролей
- > Обновление системы

**Снижение
~95%
рисков на**

Небольшие организации



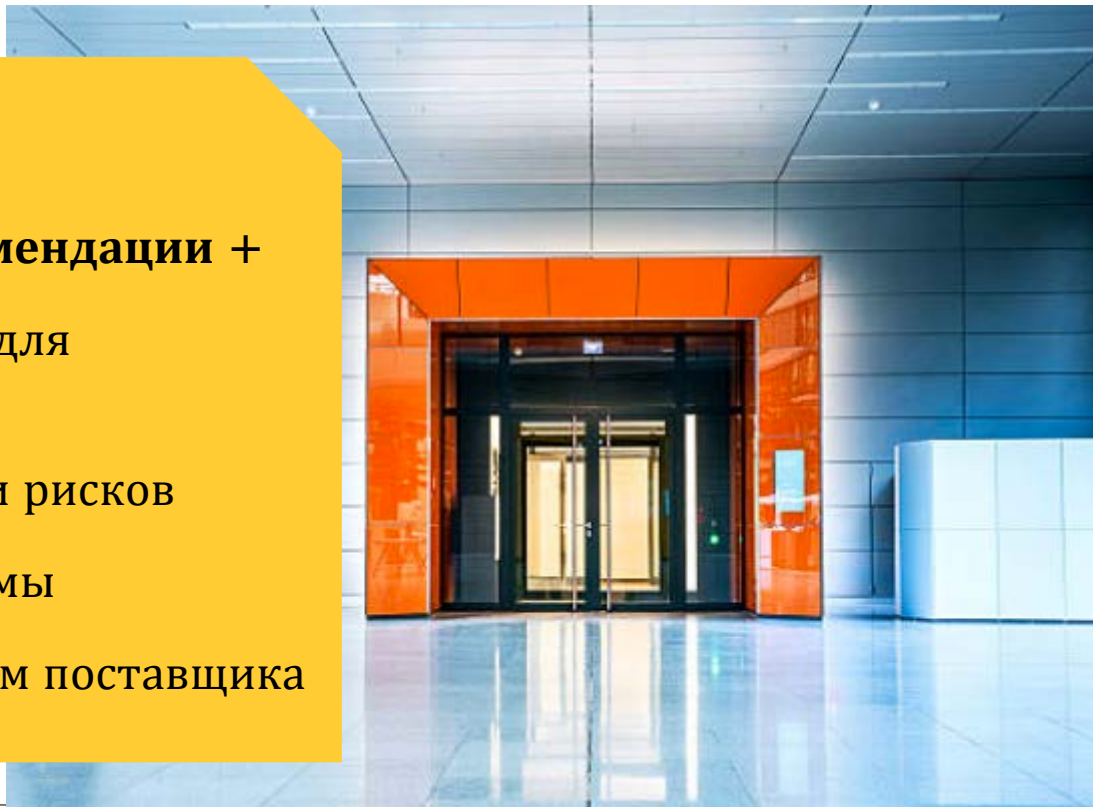
Рекомендации

- > Соблюдайте общие рекомендации
- > Используйте кодовые фразы
- > Не выводите камеру напрямую в Интернет

Рекомендации

Соблюдайте общие рекомендации +

- > Определяйте политики для видеосистем
- > Делайте базовые оценки рисков
- > Изолируйте видеосистемы
- > Следуйте рекомендациям поставщика



Рекомендации

Соблюдайте общие рекомендации +

- > Следуйте стандартам
- > Изолируйте критически важные активы
- > Работайте с доверенными, опытными партнерами



Общие ошибки, повышающие риск

Небольшие организации

- > Камера выведена напрямую в интернет
- > Пароль по умолчанию



www.axis.com

Предприятия

- > Плохая физическая защита
- > Единая учетная запись
- > Слабые пароли
- > Единая учетная запись сервера
- > Пользовательские приложения на сервере
- > Неизолированная сеть



Объекты жизнеобеспечения

- > Плохой аудит поставщиков на кибербезопасность



Кибербезопасность – это не продукт или характеристика камеры, которые можно купить и «поставить галочку», что он есть.

Это целый процесс, который выстраивается не за один день.

