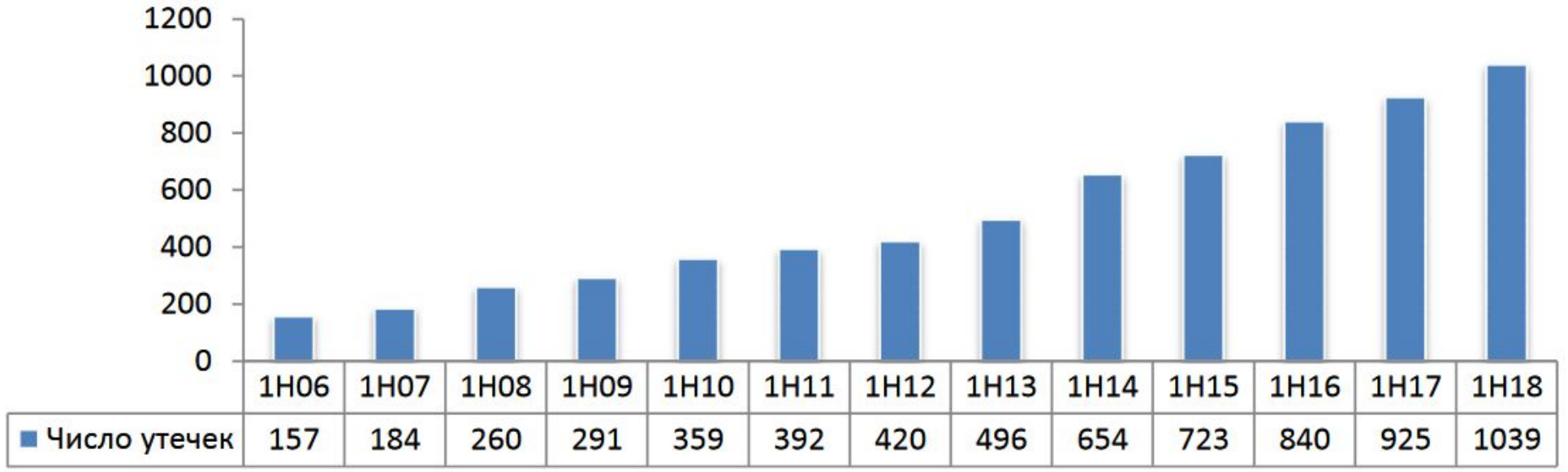
Востребованные навыки специалистов по информационной безопасности в государственных учреждениях Ставропольского края

Скубицкий Антон Витальевич

Заместитель начальника отдела обеспечения средствами связи и защиты информации Межрегионального филиала Федерального казённого учреждения «Центр по обеспечению деятельности Казначейства России» в г. Ставрополе

Глобальное исследование утечек конфиденциальной информации в 1 полугодии 2018 года (Infowatch)

За I полугодие 2018 года Аналитическим центром InfoWatch было зарегистрировано 1039 случаев утечки конфиденциальной информации (см. Рисунок 1). Это на 12% больше, чем за аналогичный период 2017 года (925 утечек).



	1H06	1H07	1H08	1H09	1H10	1H11	1H12	1H13	1H14	1H15	1H16	1H17	1H18
Число утечек	157	184	260	291	359	392	420	496	654	723	840	925	1039

Рисунок 1. Число зарегистрированных утечек информации, ½ 2006 – ½ 2018 гг.

https://www.infowatch.ru/sites/default/files/report/analytics/russ/infowatch_global_report_2018_half_year.pdf

Оценка и прогноз по расходам на информационную безопасность от компании Gartner

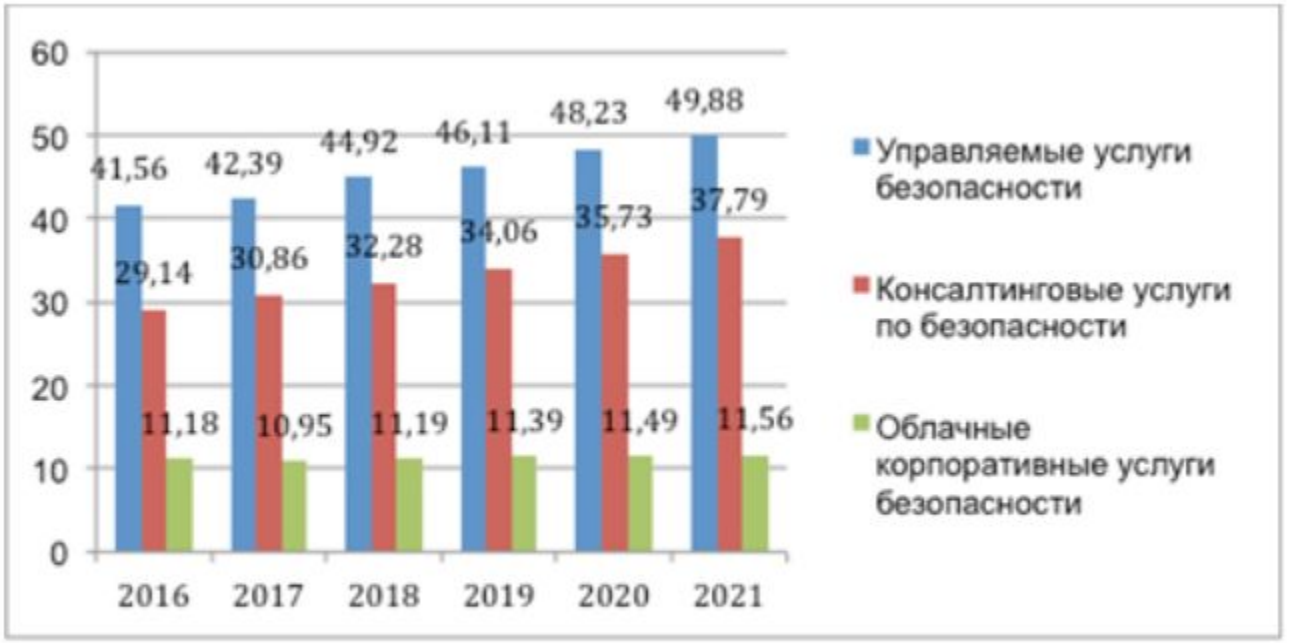
Worldwide Security Spending by Segment, 2017-2019 (Millions of U.S. Dollars)**

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	**101,544**	**114,152**	**124,116**

Source: Gartner (August 2018)

http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_(мировой_рынок)

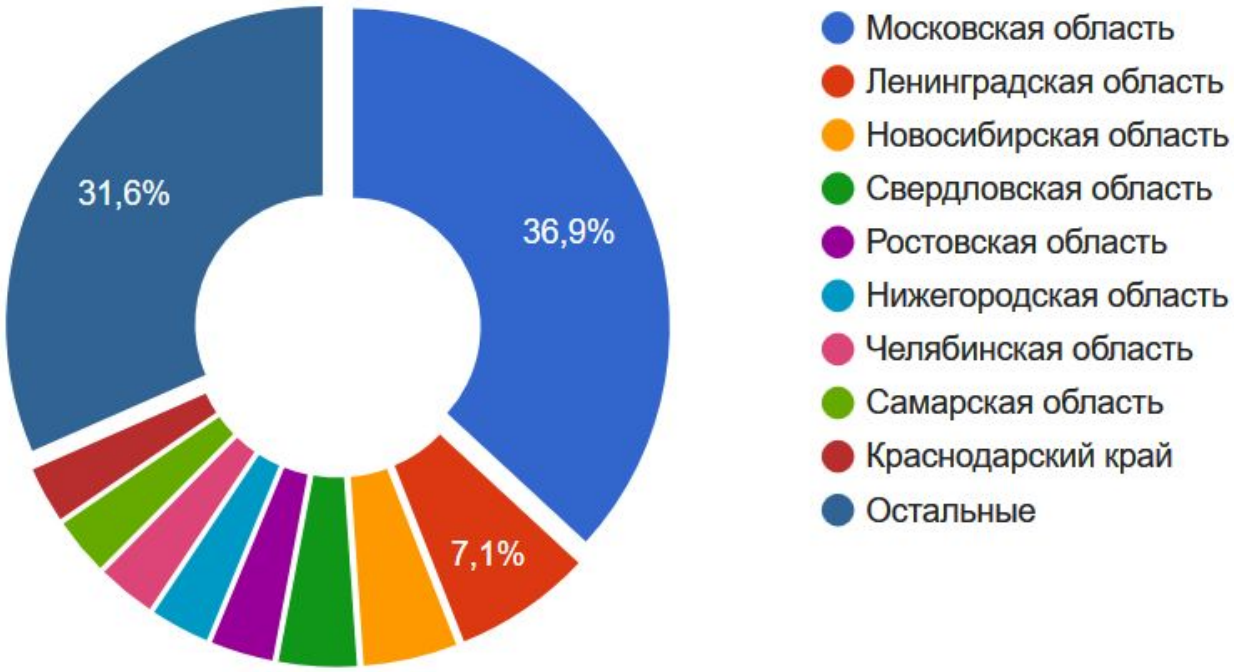
Российский рынок услуг безопасности (International Data Corporation)



Объем и прогноз развития российского рынка услуг безопасности (млн долларов)

http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_(рынок_России)

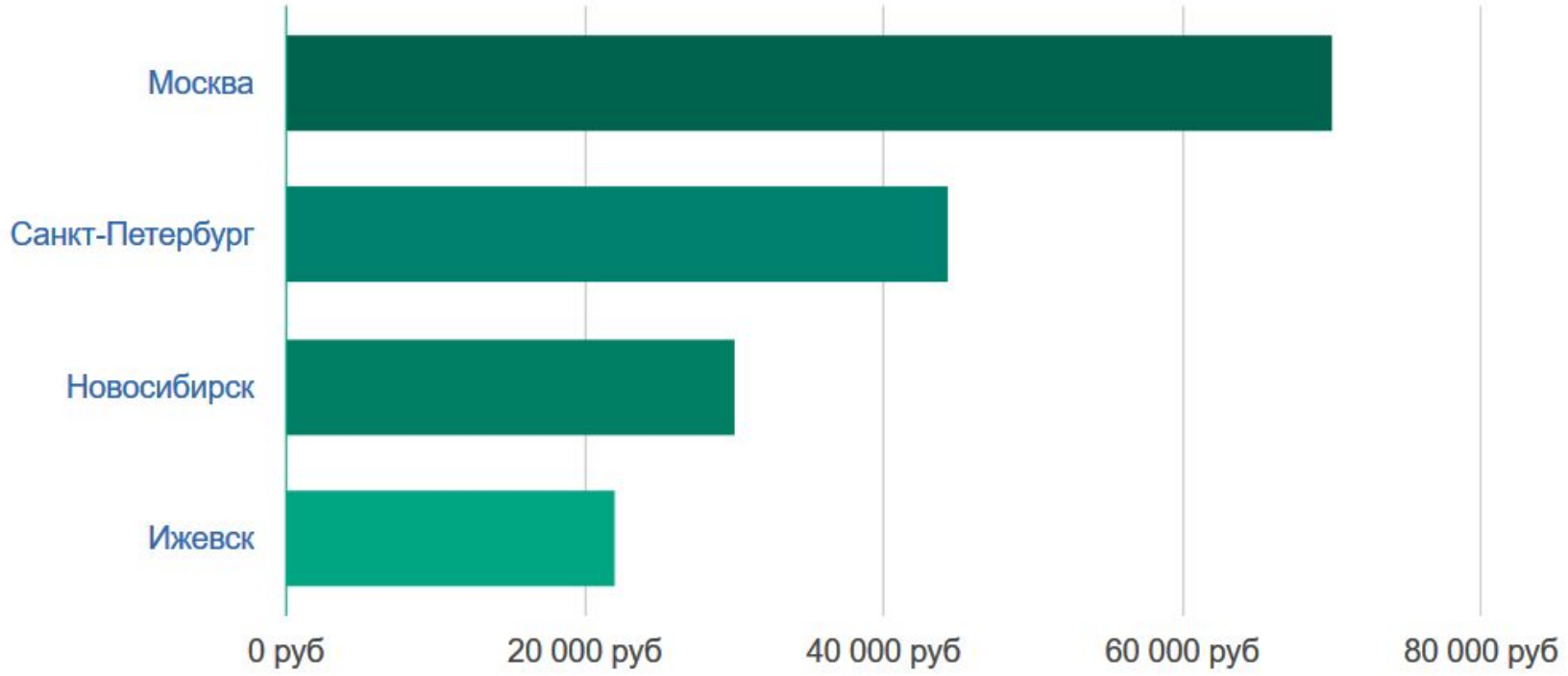
Распределение вакансии Специалист по информационной безопасности по регионам РФ



https://russia.trud.com/salary/692/67683.html

- «Силовики» (ФСБ, МО, МВД,…)
- Коммерческие организации
- Государственные организации

Уровень заработной платы: Специалист по информационной безопасности в крупных городах России



https://russia.trud.com/salary/692/67683.html

Зарплатный диапазон (Net)

Зарплатный диапазон	Регион	ИТ / Телеком (т.руб/мес.)	Промышленность (т.руб/мес.)	Финансы (т.руб/мес.)	Требования и пожелания к навыкам
1. Без опыта	Мск	45 – 60	45 – 55	45 – 57	Неполное ВО (техническое/ИТ); знание НПА и стандартов ИБ; знание стандартов шифрования; знание технологий ИБ; знание ПО и АО для ИБ
	СПб	37 – 50	37 – 45	37 – 47	
2. Минимальный опыт (от 1 года)	Мск	60 – 68	55 – 72	57 – 70	Опыт настройки и конфигурирования СЗИ; опыт проведения аудитов ИБ
	СПб	50 – 56	45 – 60	47 – 57	
3. Имеется опыт (от 2 лет)	Мск	68 – 100	72 – 100	70 – 98	ВО (техническое/ИТ); знание англ.языка (чтение тех.документации); опыт разработки регламентов и политик ИБ; опыт проведения расследований инцидентов ИБ
	СПб	56 – 82	60 – 82	57 – 80	
4. Значительный опыт (от 3 лет)	Мск	100 – 170	110 – 150	98 – 150	Наличие сертификатов ИБ; опыт реализации систем ИБ в крупных корп.сетях; опыт проектирования и разработки эксклюзивных систем и методов ЗИ
	СПб	82 – 140	82 – 125	80 – 125	
Среднерыночная ЗП	Мск	100	100	95	
	СПб	82	82	78	

http://80na20.blogspot.com/2017/10/2017.html

Региональные коэффициенты

	Специалисты	Мидл-менеджеры	Топ-менеджеры
Москва	1	1	1
Владивосток	0.75	0.80	0.85
Екатеринбург	0.67	0.72	0.77
Ижевск	0.47	0.52	0.57
Казань	0.56	0.61	0.66
Нижний Новгород	0.56	0.61	0.66
Пермь	0.55	0.60	0.65
Сочи	0.74	0.79	0.84
Сургут	0.80	0.85	0.90
Уфа	0.53	0.58	0.63
Хабаровск	0.72	0.77	0.82
Ярославль	0.57	0.62	0.67
…			

http://80na20.blogspot.com/2017/10/2017.html

Типичный функционал (специалист)

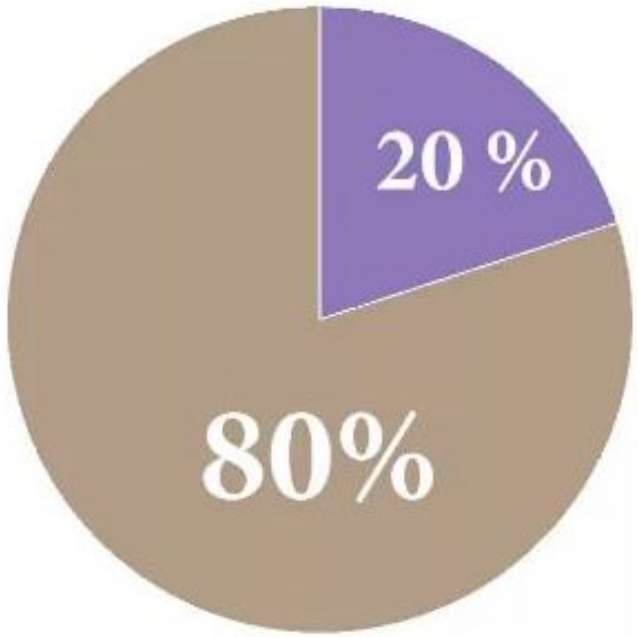
- Мониторинг и анализ состояния систем защиты информационных технологий компании, подготовка рекомендаций по их усовершенствованию
- Разработка и внедрение политик и регламентов по обеспечению защиты информации
- Подготовка и реализация технических решений по защите информации
- Контроль технического состояния систем ИБ, своевременное устранение возникающих технических проблем
- Контроль соблюдения всеми категориями пользователей требований по обеспечению ИБ
- Консультирование и обучение сотрудников мерам по обеспечению ИБ
- Анализ отчетов по случаям несанкционированного доступа, разработка методов борьбы с нарушениями
- Участие в проектах модернизации информационной инфраструктуры, закупках оборудования

http://80na20.blogspot.com/2017/10/2017.html

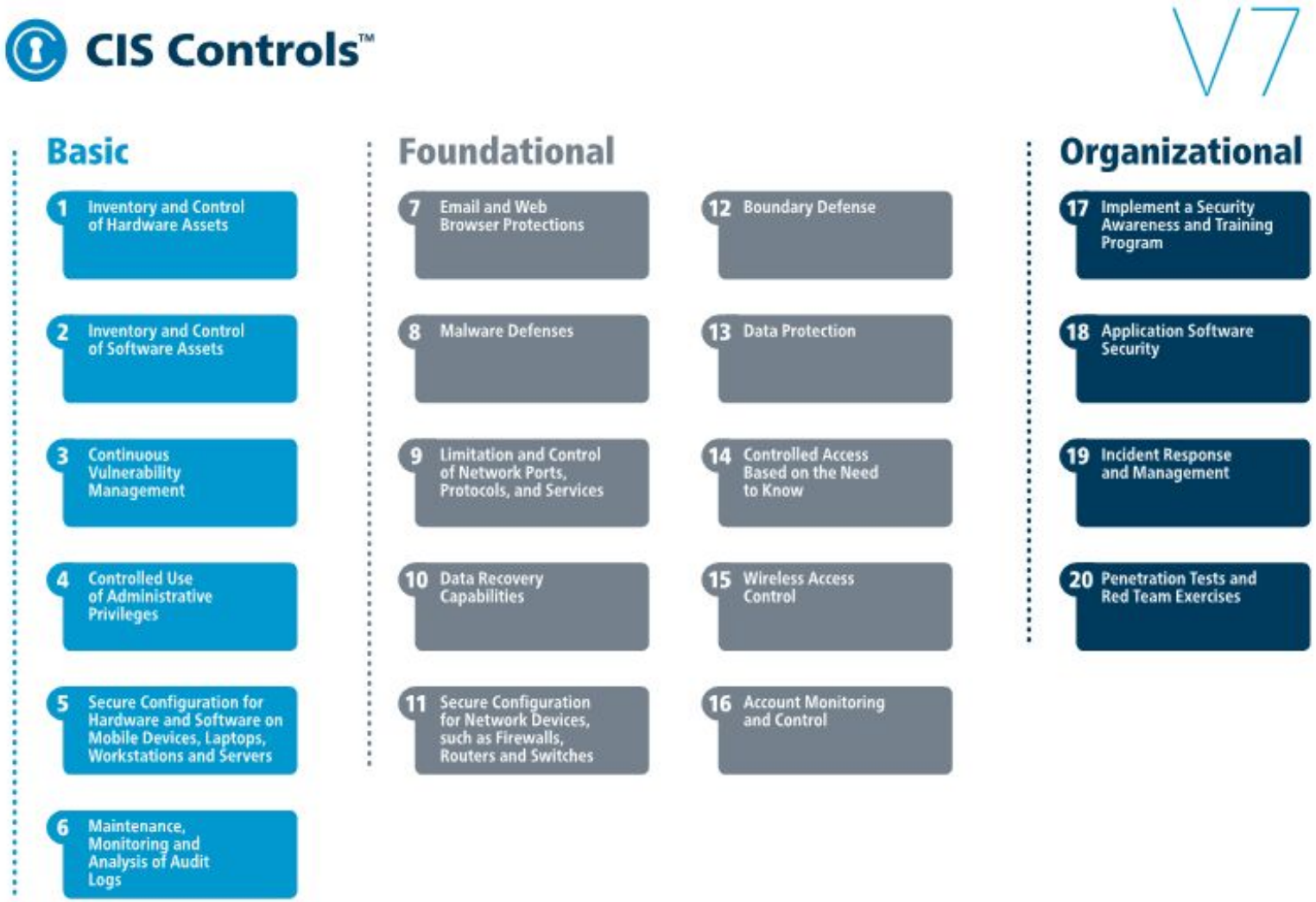
Догматичная и прагматичная ИБ

Догматичная ИБ	Прагматичная ИБ
Безопасность через страх	Оценка ИБ (риски, выгоды, возврат инвестиций)
Информационная безопасность	Cybersecurity
Защита информации	Защита бизнес-процессов
Модели угроз и нарушителя	Кейсы с расчетом TCO и ROI
Кцд	кЦД
Приказы регуляторов	«Лучшие практики»
Руководитель ИБ	Менеджер ИБ
Вся ИБ внутри организации	Присматриваемся к аутсорсингу
«Запрещено все, что не разрешено»	Разрешено с ограничениями и под контролем
Предотвращение инцидентов	Выявление и реагирование на инциденты
Внедрение СЗИ	Внедрение процессов управления и обеспечения ИБ
Защита от НСД, АВЗ, МСЭ, VPN – лучшие друзья безопасника	VM, DLP, SIEM, CASB– лучшие друзья безопасника
Мобильные устройства запрещены	Контролируем мобильных сотрудников
Облака запрещены	Мониторим и контролируем облака
Ознакамливаем с документами ИБ. Под роспись	Обучаем и повышаем осведомленность

Принцип Парето



20% усилий дают 80% результата,
а остальные 80% усилий —
лишь 20% результа



https://www.cisecurity.org/

Цикл Деминга-Шухарта (PDCA)

Тестовые стенды «Код Безопасности»

Для изучения возможностей решений "Кода Безопасности" предлагаем специально подготовленные тестовые стенды. Каждый стенд содержит образ
форматах .ovf или .vmx с предварительно установленным и настроенным соответствующим программным обеспечением, а также сопровождающий документ
и подробной инструкцией по развертыванию.

Скачать образы виртуальных машин и описание стендов можно по ссылкам ниже

Континент TLS VPN Сервер

- Скачать стенд Континент TLS VPN Сервер, 21,9 Гб;
- Скачать сопровождающую документацию с детальным описанием и подробной инструкцией по развертыванию, .pdf

АПКШ "Континент" версии 3.7

- Скачать стенд АПКШ "Континент" версии 3.7, 39,4 Гб;
- Скачать сопровождающую документацию с детальным описанием и подробной инструкцией по развертыванию, .pdf

СОВ "Континент" (АПКШ "Континент" версии 3.7, исполнение 2)

- Скачать стенд СОВ "Континент", 33,2 Гб;
- Скачать сопровождающую документацию с детальным описанием и подробной инструкцией по развертыванию, .pdf

Secret Net Studio

- Скачать стенд Secret Net Studio, 23,6 Гб;
- Скачать сопровождающую документацию с детальным описанием и подробной инструкцией по развертыванию, .pdf

vGate R2

- Скачать стенд vGate R2, 31,9 Гб.
- Скачать сопровождающую документацию с детальным описанием и подробной инструкцией по развертыванию, .pdf

https://www.securitycode.ru/products/stands/

Пожелания к наличию сертификатов ИБ

Вакансии от 12-10-2017

	HH.ru	superjob.ru
CISM	13	0
CISSP	23	1
CISA	31	1
CEH	8	0
CGEIT	3	1
CCNA	92	4

http://80na20.blogspot.com/2017/10/2017.html

Soft skills и не только

- Коммуникативные навыки (в т.ч. «слабые связи»)
- Публичные выступления
- Написание текстов, презентаций
- Английский язык
- Тайм менеджмент
- Делегирование и контроль
- Навыки работы с большими текстами
- Умение работать в коллективе

Собеседование

- Не врите
- Будьте адекватны и проявляйте заинтересованность
- Задавайте вопросы
- Следите за своими соцсетями
- Сумейте рассказать про тему дипломной работы

Не теряйте время

Спасибо за внимание!

Вопросы?