КАДРОВОЕ ОБЕСПЕЧЕНИЕ ИБ

Выполнила: Кавелина Е.М. ТЗ-13-1

ЕСТЬ ЛИ СПРОС НА УСЛУГИ СПЕЦИАЛИСТА ПО ИБ?

Найти

Специалист по информационной безопасности

> Вакансии > в Украине > Специалист по информационной безопа

Найти сейчас!

Работа Специалист по информационной безопаснос

Украине

Найдены **43** вакансии за 30 дней

IT auditor – Cyber Security – Consulting

Deloitte

Киев

Deloitte CIS is currently searching for an IT auditor in its Consulting department of our Kyiv office. We are looking for candidate to lead and

Ведущий специалист сектора к информационных рисков

Регион: Киев

Отрасль компании: Банки

Контактное лицо: Платонова Наталья

Вид занятости

Дата публикац

Если Вы:

Имеете высшее техническое образование по направлени

Обладаете опытом системного администрирования и сопр

телекоммуникационных систем не менее 3-х лет, опытом а

средств безопасности Firewall, IPS, AV, DLP.

Владеете знаниями MS Active Directory, PowerShell, OS Li

стандартов ISO 27000 и PCI DSS.

Являетесь пользователем английского языка (уровень inte

ПРИСОЕДИНЯЙТЕСЬ К НАШЕЙ КОМАНДЕ!

В Ваши функциональные обязанности будет входить:

Контроль информационных ресурсов на соответствие требованиям информа

безопасности (ИБ).

Контроль выполнения требований нормативных документов по ИБ в подразде

банка.

Администрирование средств ИБ.

Расследование инцидентов ИБ.

eva

ВЫБИРАЯ РАБОТУ,
ВЫБИРАЙ СЕБЕ СЕМЬЮ!

Инже
инфо

Регион: Дн

Отрасль к

Retail

Крупная н

"Инженер

Функцион

-монитори

-устранени

-администр

- поддер

- создани

-администр

Требовани

Опыт рабо

политик,ау

Условия:

Заработ

Социаль

Malware researcher for Imunify360.com (Remote)

Cloud Linux Inc

Днепр (Днепропетровск)

СМОТРЕТЬ ВСЕ ПОХОЖИЕ →

Другие возможности

2017-03-17 пятница

Авторская школа Наталии Байкаловой «Мастер

ФК «Шахтер» приглашает к участию в конкурсе на вакансию

«Специалист по информационной безопасности»

г. Киев

В рамках защиты коммерческой, финансовой и иной информации, связанной с деятельностью предприятия основной задачей является разработка и реализация политики информационной безопасности.

Успешному кандидату необходимы

Следующие знания:

- Знание нормативных документов по вопросам защиты информации
- Знание гражданского, уголовного и трудового прав
- Знание методов работы с информацией из Интернет-ресурсов, социальных сетей и специализированных информационных баз
- Навыки проведения внутреннего аудита информационных баз на предприятии

Технические навыки:

- знание стандартов ИБ (в первую очередь ДСТУ ISO/IEC 27001:2015, ДСТУ ISO/IEC 27002:2015, ДСТУ ISO/IEC 270005:2015) и успешный опыт их внедрения, наличие профильных сертификатов является преимуществом;
- опыт создания нормативной документации по ИБ в рамках СУИБ;
- понимание лучших мировых практик и других нормативных документов в области ИБ (NIST, SANS, BSI);

Ведущий специалист сектора контроля информационных рисков

Первый Украинский Международный Банк, ПАО / ПУМБ

Киев

СМОТРЕТЬ ВСЕ ПОХОЖИЕ →

Другие возможности

2017-03-17 пятница

Авторская школа Наталии Байкаловой «Мастер переговоров»

2017-03-18 суббота

Мастер-класс «Публичное выступление: голос, мимика, жесты»

2017-03-21 вторник

Science Rocks: встреча с археологом Эвелиной Кравченко

ВСЕ ВОЗМОЖНОСТИ →

Читайте и слушайте

Лидерство

Анатомия достижений: 7 разных мнений о том, что приводи людей к успеху

Подборка лекций TED, в которых семь спикеров делятся своими открытиями и наблюдениями, почему к людям приходит успех.

ЧИТАТЬ →

ТРЕБОВАНИЯ К СОИСКАТЕЛЮ

- ДСТУ ISO/IEC 27001:2015 ; ДСТУ ISO/IEC 27002:2015; ДСТУ ISO/IEC 270005:2015
- Firewall knowledge
- Cryptography knowledge
- Опыт работы 3-5 лет
- Наличие сертификата
- Знание технического английского (intermediate)

Ведущий специалист сектора контроля информационных рисков

Регион: Киев
Отрасль компании: Банки
Контактное лицо: Платонова Наталья

Вид занятости: полная занятость
Дата публикации: 13.03.2017

Если Вы:

Имеете высшее техническое образование по направлению «Компьютерные науки».
Обладаете опытом системного администрирования и сопровождения операционных и телекоммуникационных систем не менее 3-х лет, опытом администрирования и аудита средств безопасности Firewall, IPS, AV, DLP.
Владеете знаниями MS Active Directory, PowerShell, OS Linux, знаниями серии стандартов ISO 27000 и PCI DSS.
Являетесь пользователем английского языка (уровень intermediate).

ПРИСОЕДИНЯЙТЕСЬ К НАШЕЙ КОМАНДЕ!

В Ваши функциональные обязанности будет входить:

Контроль информационных ресурсов на соответствие требованиям информационной безопасности (ИБ).
Контроль выполнения требований нормативных документов по ИБ в подразделениях банка.
Администрирование средств ИБ.
Расследование инцидентов ИБ.

Воля
Киев

Системный администратор, специалист по информационной безопасности
Пинакот, ООО
20000 грн. Киев

Главный специалист отдела проверок и противодействия мошенничеству (SQL, PHP)
Forward Bank
Киев

Специалист по ИТ безопасности
DATAS TECHNOLOGY
Киев

Инженер по ИТ-безопасности
ИТ-Интегратор
Киев

СМОТРЕТЬ ВСЕ ПОХОЖИЕ →

Другие возможности

2017-03-17 пятница

БОЛЬШАЯ ЧЕТВЕРКА

Образование

Опыт

Профессиональный рост

Образ жизни

ОБРАЗОВАНИЕ

- **Специальность, которая связана с автоматизацией, программированием, математикой.**
- **Технический английский**
- **Криптография**
- **Высшая математика, теория вероятностей**
- **Опыт работы и умение обращаться с железом**
- **Системное администрирование**
- **Архитектура сети**

ОПЫТ

- На выходе из ВУЗа, будущий безопасник особо не востребован. Причиной этому является то, что в данной сфере огромную роль играет опыт, нужно четко и точно знать, в какой ситуации принимать надлежащие меры и как поступать. Лучше всего обучаться и проходить практику в компании, в которой предполагаете дальнейший рост.
- Так же с большой охотой берут людей с опытом работы в госучреждениях, полиции, СБУ.

ОБРАЗ ЖИЗНИ

- **Работа безопасника связана с большим количеством ответственности и профессиональными рисками. Подобная работа часто накладывает отпечаток на образ жизни.**

- **Во-первых, ее не принято афишировать, не принято разглашать подробности о буднях безопасника, график чаще всего ненормированный .**
- **Во-вторых, вполне возможны ограничения по выездам за границу.**

ПРОФЕССИОНАЛЬНЫЙ РОСТ

- **Каждый день нужно выделять около часа на образование: это единственный шанс оставаться в целом подготовленным к тому, что происходит с технологиями. Нужно постоянно читать конкретику по известным ситуациям взломов, осваивать новые системы — и при этом всё время думать как злоумышленник снаружи.**

- **Разумеется, в форме нужно поддерживать не только себя, но и свой отдел, а также вообще всех людей в компании. Здесь два простых принципа — аудиты-проверки и учебные тревоги.**

ЗНАНИЯ И УМЕНИЯ

- **иметь представление: о системе национальной безопасности Украины; об основных подходах к определению понятия "информационная безопасность", "информационная война", "информационная борьба", "информационное оружие";**

ЗНАНИЯ И УМЕНИЯ

- **знать**: принципы, методы, системы и средства обеспечения информационной безопасности Украины; формальные модели, лежащие в основе систем обеспечения информационной безопасности, и их теоретические основы; стандарты по оценке защищенных систем и их теоретические основы; принципиальные отличия требований к системам обеспечения информационной безопасности в различных сферах деятельности;

ЗНАНИЯ И УМЕНИЯ

- **уметь**: применять системный подход к обеспечению информационной безопасности в различных сферах деятельности; проводить анализ автоматизированных систем с точки зрения обеспечения информационной безопасности; разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и теоретические основы; применять стандарты по оценке защищенных систем при анализе и проектировании систем защиты информации в автоматизированных системах;

ЗНАНИЯ И УМЕНИЯ

- **владеть: навыками разработки и анализа моделей и политики безопасности; элементами технологии разработки систем защиты информации в автоматизированных системах;**

СЕРТИФИКАЦИЯ

- **В результате повышенного внимания к вопросам информационной безопасности растет потребность компаний в квалифицированных кадрах. Одним из критериев оценки квалификации специалиста является наличие у него того или иного сертификата.**

CISSP
CISA
CRISC
CISM

Cisco
Microsoft

СЕРТИФИКАЦИЯ

- **CCNA** - для подтверждения и получения знаний построения сетей ...)
- **CISA, CISSP, CISM** - для подтверждения и получения знаний лучших практик по ИБ
- сертифицированный специалист по внедрению/аудиту ISO 27000
- для подтверждения и получения знаний по аудиту ИБ и подготовке к сертификации по ISO 27000
- **CEH** - для подтверждения и получения базовых знаний по пентесту
- **MsSQL** - для подтверждения и получения знаний по работе с базой данных
- **Microsoft Server administrator** - для подтверждения и получения знаний по работе с серверным оборудованием
- **VMvare** - для подтверждения и получения знаний по работе с виртуальными машинами

Сертификация специалистов по информационной безопасности

	CISM	CISA	CGEIT	CRISC	CFC (CSX)	CISSP	SSCP	Security+
Полное название	Certified Information Security Manager	Certified Information Systems Auditor	Certified in the Governance of Enterprise IT	Certified in Risk and Information Systems Control	Cybersecurity Fundamentals Certificate	Certified Information Systems Security Professional	Systems Security Certified Practitioner	CompTIA Security+
Ассоциация	ISACA	ISACA	ISACA	ISACA	ISACA	(ISC)2	(ISC)2	CompTIA
Сайт	www.isaca.org	www.isaca.org	www.isaca.org	www.isaca.org	www.isaca.org	www.isc2.org	www.isc2.org	www.comptia.org
Стоимость	440 $ *	440 $ *	440 $ *	440 $ *	150 $	599 $	250 $	302 $
Формат экзамена	Тест письменно на площадке УЦ (3 раза в год)	Тест письменно на площадке УЦ (3 раза в год)	Тест письменно на площадке УЦ (2 раза в год)	Тест письменно на площадке УЦ (2 раза в год)	Тест онлайн на своей площадке	Тест письменно или онлайн на площадке УЦ	Тест письменно или онлайн на площадке УЦ	Тест онлайн на площадке УЦ
Необходимый опыт	5 лет	5 лет	5 лет	3 года	Нет	5 лет	1 год	2 года
Длительность экзамена	4 часа	4 часа	4 часа	4 часа	2 часа	6 часов	3 часа	1,5 часа
Кол-во вопросов теста	200	200	150	150	75	250	125	90
Проходной балл	450 + (шкала 200-800)	450 + (шкала 200-800)	450 + (шкала 200-800)	450 + (шкала 200-800)	65% +	700 + (из 1000)	700 + (из 1000)	750 (шкала 100-900)
Домены	1. Information Security Governance (24%) 2. Information Risk Management and Compliance (33%) 3. Information Security Program Development and Management (25%) 4. Information Security Incident Management (18%)	1. The Process of Auditing Information Systems (14%) 2. Governance and Management of IT (14%) 3. Information Systems Acquisition, Development, and Implementation (19%) 4. Information Systems Operations, Maintenance and Support (23%) 5. Protection of Information Assets (30%)	1. Framework for the Governance of Enterprise IT (25%) 2. Strategic Management (20%) 3. Benefits Realization (16%) 4. Risk Optimization (24%) 5. Domain 5: Resource Optimization (15%)	1. IT Risk Identification (27%) 2. IT Risk Assessment (28%) 3. Risk Response and Mitigation (23%) 4. Risk and Control Monitoring and Reporting (22%)	1. Cybersecurity Concepts (10%) 2. Security of Network, System, ApplicaDon, & Data (40%) 3. Cybersecurity Architecture Principles (20%) 4. Incident Response (20%) 5. Security of Evolving Technology (10%)	1. Security and Risk Management (Security, Risk, Compliance, Law, Regulations, Business Continuity) 2. Asset Security (Protecting Security of Assets) 3. Security Engineering (Engineering and Management of Security) 4. Communications and Network Security (Designing and Protecting Network Security) 5. Identity and Access Management (Controlling Access and Managing Identity) 6. Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing) 7. Security Operations (Foundational Concepts, Investigations, Incident Management, Disaster Recovery) 8. Software Development Security (Understanding, Applying, and Enforcing Software Security)	1. Access Controls 2. Security Operations and Administration 3. Risk Identification, Monitoring and Analysis 4. Incident Response and Recovery 5. Cryptography 6. Networks and Communications Security 7. Systems and Application Security	1. Network Security (20%) 2. Compliance and Operational Security (18%) 3. Threats and Vulnerabilities (20%) 4. Application, Data and Host Security (15%) 5. Access Control and Identity Management (15%) 6. Cryptography (12%)
Подтверждение	Каждые 3 года или 120 CPE	Каждые 3 года или 120 CPE	Каждые 3 года или 120 CPE	Каждые 3 года или 120 CPE	Нет	Каждые 3 года, или 120 CPE	Каждые 3 года или 60 CPE	Каждые 3 года или 50 CEU

• - ранняя регистрация для членов ISACA

CISSP

- **Certified Information Systems Security Professional** – это вендорнезависимая сертификация по информационной безопасности от некоммерческой организации International Information Systems Security Certifications Consortium, более известной как (ISC)²

- Сертификация CISSP в первую очередь предназначена для консультантов, аудиторов, архитекторов, аналитиков и управленцев в области информационной безопасности (ИБ).
  CISSP относят к числу высших сертификаций в области ИБ.

- **Сертификация включает в себя 10 тем (доменов):**

  - Access Control
  - Telecommunications and Network Security
  - Information Security Governance and Risk Management
  - Software Development Security
  - Cryptography
  - Security Architecture and Design
  - Operations Security
  - Business Continuity and Disaster Recovery Planning
  - Legal, Regulations, Investigations and Compliance
  - Physical (Environmental) Security

ПОДГОТОВКА К СЕРТИФИКАЦИИ УКРАИНА

- **Компания ISSP | Information Systems Security Partners, официальный тренинг-партнер компании (ISC)2 проводит набор группы на авторизованное обучение по направлению CISSP (Certified Information Systems Security Professional).**

  Длительность 5 дней

  Г. Киев

Или

- **Перевод 5-го издания книги Шон Харрис "CISSP All-In-One Exam Guide"**

ПОЛНОЕ • РУКОВОДСТВО

CISSP

#1

РУКОВОДСТВО ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

ПЯТАЯ РЕДАКЦИЯ

Полностью охватывает все 10 доменов курса подготовки специалистов по безопасности информационных систем

▪

Отлично подходит как для подготовки к экзамену CISSP, так и в качестве руководства для самостоятельного изучения предмета «Безопасность информационных технологий»

▪

Содержит примеры вопросов экзамена CISSP с подробным объяснением ответов

ШОН ХАРРИС
CISSP

ПЕРЕВОД: DORLOV.BLOGSPOT.COM V1.0

ВУЗЫ УКРАИНЫ

- Днепропетровский национальный университет им. О. Гончара (ДНУ)
- Национальная академия Службы безопасности Украины
- Национальный авиационный университет (НАУ)
- Национальный аэрокосмический университет им. Н.Е. Жуковского «Харьковский авиационный институт»
- Национальный технический университет Украины "Киевский политехнический институт" (НТУУ КПИ)
- Одесская национальная академия связи им. А. Попова (ОНАС)
- Учебно-научный институт информационной безопасности Национальной академии Службы безопасности Украины
- Государственный университет телекоммуникаций (ДУТ)

ПРОЦЕДУРА ПРИЕМА НА РАБОТУ

- **Полная проверка СБ организации. Проверка на подлинность всех существующих документов, проверка счетов, кредитных историй, обязательны рекомендательные письма от бывших работодателей, проверка трудовой книги, проверка по формальным и неформальным базам, мониторинг прошлого, проверка на детекторе лжи (неофициально), ряд собеседований (отдел кадров, начальник СБ, руководитель), моделирование кризисных ситуаций и мониторинг реакции испытуемого, подготовка ряда документов, четко регламентирующих ситуации, которые могут сложиться при уходе данной должности и где прописана ответственность каждой из сторон.**

ПРОЦЕДУРА УВОЛЬНЕНИЯ

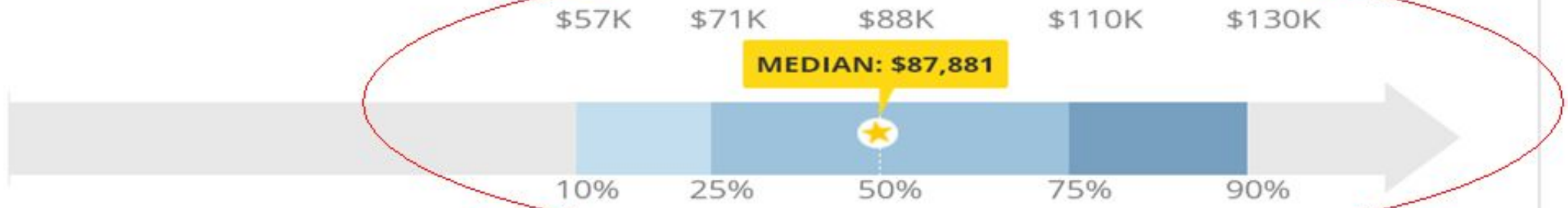
- **К сообщению сотруднику об увольнению лучше подготовится заранее, нужно смоделировать ситуацию. И быть готовым к любому развитию событий. Обязательно сразу же отозвать права аккаунта администратора, отключить служебные учетные записи, сменить пароли. Так же лучше ограничить доступ на территорию, вскрыть все сейфы, изъять все служебные носители информации, принять все журнальные отчеты о служебной деятельности сотрудника. Обеспечить правильное оформление всей соответствующей документации, подписке о неразглашении. Так же не будет лишним напомнить об уголовной ответственности, которую сотрудник несет за любое нарушение, проистекающее в утечку информации**

СРЕДНЯЯ ЗАРПЛАТА

Украина	Россия	США
~20 000 грн	~ 52000 руб (80 000 руб Москва)	~7500 $ (198 000 грн)

The average salary for a Security Engineer is $87,881 per year. A skill in Computer Security is associated with high pay for this job. Most people with this job move on to other positions after 20

Read More

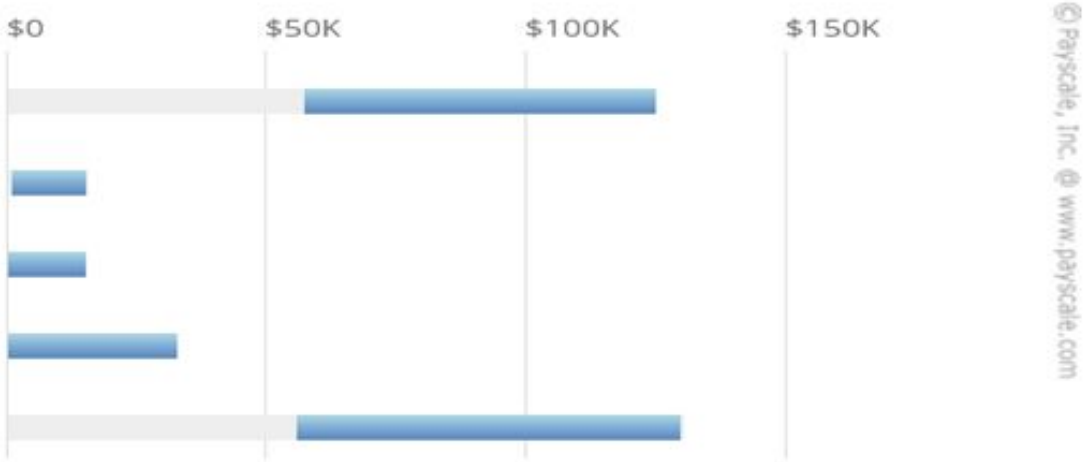


Add this chart to your site: 640px 300px

Show Hourly Rate

+ city + experience + skill job

National Salary Data (?)	
Salary	$57,254 - $125,073
Bonus	$993 - $15,584
Profit Sharing	$197.27 - $15,067
Commission	$32,500
Total Pay (?)	**$55,887 - $130,415**



Country: United States | Currency: USD | Updated: 18 Jan 2017 | Individuals Reporting: 1,015

ИСТОЧНИКИ

- Макаров В. Е. ; «**Социальные основы информационной безопасности деловой организации: Монография» , с. 57-58**
- pressa.ru ; электронный журнал «**Директор информационной службы», выпуск 04-2013, с. 62-63**
- Панкратьев В., статья «**Процедура приема и увольнения сотрудников с позиции безопасности»**
- **https://habrahabr.ru/company/it/blog/196638/**
- **https://rabota.ua/zapros/специалист-по-информационной-безопасности**
- **https://habrahabr.ru/company/croc/blog/190300/**
- **https://www.superjob.ru/research/articles/111958/specialist-po-informacionnoj-bezopasnosti/**