Приложение к рабочей программе дисциплины (практики)

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН)

Инженерная академия

(наименование основного учебного подразделения)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

ИНОСТРАННЫЙ ЯЗЫК В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

54.03.01 ДИЗАЙН

(код и наименование направления подготовки/ специальности)

Освоение дисциплины (практики) ведется в рамках реализации основной профессиональной образовательной программы (ОП ВО, профиль/ специализация):

Дизайн городской среды

(направленность (профиль) ОП ВО)

Москва, 2026

1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

1. Виды контроля по периодам обучения

Контрольная работа
Темы 1-2. «Категория наклонения. Сослагательное наклонение»
Вариант 1

Задание 1. Переведите следующие предложения на английский язык.
Вам давно пора обратиться к зубному врачу.
Даже если бы вы позвонили мне вчера, я не смог бы прийти.
Обидно, что я не увижу вашу выставку; меня уже в это время здесь не будет.
Если бы я был художником, я бы обязательно нарисовал портрет этого человека.
Жаль, что ты не пошел с нами в театр. Я уверена, тебе бы понравился спектакль.
Если бы поезд вышел вовремя, он прибыл бы в Москву завтра рано утром.
Режиссер распорядился, чтобы во время репетиции в зал никого не впускали.
Вам не кажется странным, что она забыла о таком важном деле?
Он посмотрел на меня так, будто никогда раньше меня не видел.
Мой совет вам – сказать несколько слов об авторе, прежде чем вы начнете говорить о самой книге.
Что бы вы сделали, если бы я обратился к вам за советом?
Они бы заметили эту ошибку, если бы были более внимательными.
Если бы только мы могли убедить его не уезжать!
Почему вы не позвонили мне? Я бы пришел и помог вам.
Я решил рассказать сестре о своем намерении уехать, чтобы она не волновалась, когда утром обнаружит, что меня нет.

Задание 2 . Перефразируйте следующие предложения с использованием средств выражения нереальности в придаточных предложениях.

They did this hardest job as if playing an amusing game.
But for his tender eyes his face would seem almost cruel.
It is a pity that you were not present at our party yesterday.
The competition would have taken place even in cold weather.
He thought it time to close the debate.

Задание 3. Дайте развернутый ответ на следующий вопрос: What would you do if today were the first day after you've passed all your winter exams?

Контрольная работа
Темы 1-2. «Категория наклонения. Сослагательное наклонение»

Вариант 2.

Задание 1. Переведите следующие предложения на английский язык.

Не пора ли нам обратить серьезное внимание на этот вопрос?
Он бы выполнил это задание, даже если бы оно было вдвое труднее.
Жаль, что я не смогу провести с вами эти летние каникулы. Я уезжаю на стажировку в США.
Если бы вы послушали совета врача, вы давно бы выздоровели и смогли бы пойти с нами на концерт.
Она пожалела, что упомянула мое имя в его присутствии. Я уверен, что иначе он никогда и не вспомнил бы обо мне.
Если бы он поступил в институт четыре года назад, он уже окончил бы его в будущем году.
Комиссия потребовала, чтобы этот вопрос обсудили на открытом собрании.

Странно, что вы не поняли лекцию, она была очень простая.
Что с вами? У вас такой вид, будто вам нехорошо.
Его предложение сводилось к тому, чтобы новые факты также были приняты во внимание.
Если вдруг снова приедете в наш город, непременно загляните к нам.
Вы были бы недовольны, если бы я не пришел?
Если бы я слышал прогноз погоды! Я бы захватил плащ.
Он очень аккуратен и ни за что не опоздал бы без причины.
Она сделала вид, будто ищет что-то в бумагах, чтобы никто не заметил ее волнения.

Задание 2 . Перефразируйте следующие предложения с использованием средств выражения нереальности в придаточных предложениях.

I am sorry to have bothered you about such trifles.
The pudding would taste better for some more plums.
I should have never believed it, but I saw it with my own eyes.
After the bath he felt as if born anew.
I would never complain in your place.

Задание 3. Дайте развернутый ответ на следующий вопрос: What would you do if today were the first day of your summer holidays?

Контрольная работа
Темы 3-4. «Модальные глаголы. Модальное слово, частица, предлог, союз и междометие»

Вариант 1

Задание 1. Переведите следующие предложения на английский язык.

Если бы мы поехали вечерним поездом, мы могли бы опоздать на пароход.
Возможно, она была на концерте, но я ее не видел.
Напрасно ты сказала ей об этом. Тебе следовало бы промолчать.
Не может быть, чтобы он не слышал о нашем решении.
Делегация должна была прилететь 14-го ноября, но из-за плохой погоды рейс пришлось отложить.
Незачем вам было приезжать так рано. Конференция должна начаться только через 2 часа.
Он, должно быть, не приготовил перевод заранее. Теперь ему, вероятно, придется провести в библиотеке весь завтрашний день.
С какой стати я должна идти в магазин? Ты мог бы сам купить что-нибудь к обеду, ты же знал, что я неважно себя чувствую.
Мне ничего другого не оставалось, как признать свою ошибку.
Как ты смеешь так разговаривать с матерью?
Ты, наверное, проголодался. Принести тебе чашку чая и бутерброд
Ты смог найти нужную книгу? Спроси у Джона. Он должен знать, в каком книжном она продается.
Он сказал, что ему придется уехать через несколько дней, но мы и слушать не хотели.
Мне жаль, что он так плохо думает обо мне.
«Стой где стоишь!»,- в бешенстве крикнула она. Я понял, что мне лучше послушаться.

Задание 2 . Выполните частичный перевод следующих предложений.

I had never ceased to write to Peggotty, but (должно быть прошло) seven years since we had met.
(Могу ли я сделать) as I like or (я должна сделать) as you like?
“I’m sorry about Mabel,” said Isaac. Lanny shrugged: “I suppose it (должно было случиться).”
Somebody has been talking; (кто бы это мог быть)?
Frequently he (можно было застать) in the garden bent over his flowers (2 variants).

Задание 3. Составьте ситуации с использованием следующих выражений:
shouldn’t have gone

needn’t have gone

Контрольная работа
Темы 3-4. «Модальные глаголы. Модальное слово, частица, предлог, союз и междометие»

Вариант 2

Задание 1. Переведите следующие предложения на английский язык.

Ты такой неуклюжий! Ты ведь чуть не разбил мамину любимую вазу!
Возможно, он приготовил перевод заранее.
Тебе не стоило так себя вести. Она, должно быть, обиделась.
Неужели вы им не сообщили о его приезде? Вам следовало бы сразу им позвонить.
Андрей должен был приехать вчера, но его сестра позвонила и сказала, что он не сможет приехать.
Оказалось, что я зря стоял в очереди за билетами: я мог бы заказать их по телефону.
Ему даже не нужно было называть своей фамилии: его и так все хорошо знали.
Я вчера ходила в кино. И как ты думаешь, кого я там встретила? Конечно Анну!
Скажи ему, что он мог бы быть более внимательным к своим старым друзьям.
Не переживай. В конце концов, дела обстоят не так уж плохо.
Может тебя проводить до дома? Я просто не могу оставить тебя одну.
Он не осмеливается просить тебя об этом. Он думает, что ты все еще злишься.
Не беспокойтесь, я обещаю устроить все так, как вы хотите.
Не понимаю, с чего это он решил сюда прийти.
Я простоял два часа под навесом, но дождь и не думал прекращался.

Задание 2 . Выполните частичный перевод следующих предложений.
“Now listen to me!” he said; “I’ll tell you a few things that you (должен был бы спросить) before starting out.”
Mr. Barkis, the carrier, (должен был заехать) for me in the morning at nine o’clock.
(Незачем было волноваться), everything has turned out all right.
Lanny opened his eyes and looked at the smiling young woman, who leaned over him. (Это, вероятно, Мейбл).
I believe he was always afraid they (могут посмеяться) at him.

Задание 3. Составьте ситуации с использованием следующих выражений:
Should have come
Was to have come

Контрольная работа
Темы 5-7. «Неличные формы глагола. Инфинитив. Герундий. Причастие»

Вариант 1.
Задание 1. Вставьте *“to”* где необходимо

Do you think I plan … spend the rest of my life in the same situation? I’d rather … die!
I’ve never known him … be so jealous.
She could not help but … feel a little chocked for breath.
He gave a quick grin that made his lean twisted face … look more lean and twisted than ever.
I felt my blood … freeze.
Ever since I came into this silly house I have been made … look like a fool.
Not … go back was awful.
You’d better … take me back to Oxford.
I would … die sooner than … ask him for another penny.
Why not … start up our own business?

Задание 2. Раскройте скобки, поставьте глагол в соответствующую форму (инфинитив или герундий).

He is capable (to do) things you would least expect of him.
I regret (to say) I am not coming.
He would not stop (to ask) questions until he thought he was clear about everything.
She showed no sign (to impress).
He hated (to remind) people of their duties or (to remind) of his.
Mr. Snodgrass was the first (to break) the astonished silence.
The equipment must go through a number of tests before (to install).
You never mentioned (to speak) to them on the subject.
You can't be serious (to make) me such a proposition.
We called after him, but he didn't even stop (to turn) his head.
This is not the way (to talk).
She is much too old (to go) climbing as she used to.
Mary deserves (to punish).
Why (to go) in that matter at all.
You can hardly count (to find) everything as you would like it to be.

Задание 2. Вставьте not или without перед формой глагола, оканчивающегося на – ing.
… waiting for an answer, he turned round and walked out.
I tried to catch his eye but he sat motionless, … looking in my direction.
They jumped at the proposition, … thinking of the consequences.
The wind had been blowing for many days … seeming to stop.
The young man asked me all kinds of questions … concealing his curiosity.
He never signed a paper … having thoroughly read it out.
The door stood ajar, and we entered … knocking.

Задание 3. Переведите следующие предложения на английский язык.

Этот шанс означает движение вперед.
Купить эти акции все равно, что выбросить деньги на ветер.
Мягко говоря, он оказался ненадежным человеком.
Он уехал, чтобы уже никогда не вернуться.
Я очень удивился, обнаружив, что он продал все, что у него было, и уехал в деревню. Думаю, когда-нибудь он пожалеет, что сделал это.
Бесполезно просить его сделать скидку.
Ему важно произвести хорошее впечатление на собеседника.
Я не могу позволить себе купить такую дорогую машину.
Кажется, он работает над проектом уже много недель, и достиг определенных результатов.
Ты пробовал дать объявление в газету?
Я боюсь сдавать экзамены, потому что боюсь получить плохую оценку.
Мы слышали, что он проработал здесь до пенсии.
Я попросил секретаря напечатать три письма, и еще я попросил проинформировать меня о приезде делегации.
Откровенно говоря, полагают, что цены на нефть вырастут на 15%.
Вылезая из машины, я споткнулась и упала.
Я вошел и увидел, что все было перевернуто вверх дном.
Невозможно убедить его согласиться на наш план. Кажется, он просто не понимает, чего мы хотим.
Как насчет того, чтобы сделать стрижку?
Я против того, чтобы назначать Дэвида финансовым директором.
И что еще хуже, я чувствовал, что он будет отрицать, что совершил это преступление.

Контрольная работа
Темы 5-7. «Неличные формы глагола. Инфинитив. Герундий. Причастие»

Вариант 2

Задание 1. Вставьте *"to"* где необходимо .
You know there's nobody in the world I would rather … work with or … have great respect for.
She opened the iron gateway and made me … enter.
I want … look at him and hear him … talk.
Abe let the hammer … drop out of his hands and … fall on the step.
I thought that I had better … try … speak openly myself.
All I want … do is … help you.
We can't get them … prepare the report.
They ought … have asked my advice.
I knew that … be true.
Alice was never heard … behave like this.

Задание 2. Раскройте скобки, поставьте глагол в соответствующую форму (инфинитив или герундий).
I regret (to miss) the show.
He is quite able (to take care) of himself.
I don't like your way (to talk).
After saying a few words about the author himself, the lecturer went on (to speak) of his works.
Mary deserves (to punish).
It's no use (to argue) when the matter is settled.
He had some difficulty (to control) his temper.
I am glad (to introduce) to you.
Look how animated they are! It must be nice (to dance) like that.
She was eagerly looking forward (to give) the leading part to play that she was greatly disappointed (not even to offer) it.
His time was up, but he still went on (to talk)
I am sorry (to disappoint) you but I did not mean anything of the kind.
I hate (to bother) you, but the man is still waiting (to give) a definite answer.
They didn't show the slightest desire (to accompany) us.
They don't recommend (to visit) this exhibition

Задание 3. Раскройте скобки, поставьте глагол в соответствующую форму (инфинитив или герундий).

… waiting for an answer, he turned round and walked out.
I tried to catch his eye but he sat motionless, … looking in my direction.
They jumped at the proposition, … thinking of the consequences.
The wind had been blowing for many days … seeming to stop.
The young man asked me all kinds of questions … concealing his curiosity.
He never signed a paper … having thoroughly read it out.
The door stood ajar, and we entered … knocking.

Задание 3. Переведите следующие предложения на английский язык.

Проще говоря, я хочу, чтобы все сделали так, как я сказал.
Войдя в свой кабинет, босс первым делом приказал принести кофе.
И что еще хуже, я чувствовал, что он был прав.
Когда я проходил по коридору, я видел, что Мэри показывала посетителям завод.
Полагают, что товар был застрахован неделю назад.
Сказать по правде, я не помню, чтобы я говорила что-либо подобное на конференции.
Я сожалею, что ушла со старой работы.
Ничто не сможет удержать меня от разработки этого проекта.
Мы боимся вкладывать деньги в российскую промышленность, т.к. мы боимся потерять свои деньги.
Я тебя с трудом понимаю. Но я вижу, что с тобой бессмысленно спорить сейчас.
Для него важно запомнить все цифры, упоминаемые в материале.

Я слышал, как в толпе упомянули имя моего друга.
Казалось, наш босс все понял уже давно.
Сдав все документы в срок, Майк начал готовиться к вступительным экзаменам.
Воспитанный в тишине и покое, он тяжело привыкал к городской жизни.
Короче говоря, наш план состоит в том, чтобы вытеснить конкурентов с рынка.
Как насчет того, чтобы продолжить образование за границей?
Невозможно начать новую рекламную компанию, так как мы потратили все деньги на покупку нового оборудования.
А я уже и забыл, что мы познакомились когда-то.
И что ещё хуже, я боюсь идти на экзамен, потому, что боюсь провалиться.

Контрольная работа
Темы 8-10. «Синтаксис. Пунктуация. Речевой этикет»
Вариант 1.

Задание 1. Определите тип семантических отношений между элементами сложных предложений (координация, субординация, предикация).

Polly will be offended if you go off to a hotel instead of accepting her hospitality.
There were muffled voices and footsteps, and the door opened on a plump middle-aged woman in slacks and a hand-knitted yellow sweater.
She was trembling as she stopped talking.

Задание 2. Подчеркните союзы, используемые для присоединения придаточных времени к главному предложению.
I can be happy anywhere as long as I'm with you.
"Just wait till Dad gets home", she shouted without thought.
It's a long time since I've seen you boys.
I suggest to him a course of lectures on native policy, that sort of thing, before they arrive in the country.

Задание 3. Дополните следующие предложения, раскрыв скобки.

I wondered what… (to mean)
I understand they… (to come)
I don't see why … (to apologize)
You remember how … (to promise)
I know that… (to return)
I told him what … (to discuss)
I feel that … (to know)
I take it that …. (to be in the know).
I wish we … (to stay)
He suggested … (to have lunch).

Задание 4. Переведите следующие предложения на английский язык, используя the Complex Object and Complex Subject.

Известно, что товар был застрахован в прошлую пятницу.
Она ожидает, что он придет сюда и поможет ей переустановить Word.
Я предполагаю, что нашему боссу лет 50.
Почему вы не попросили, чтобы вам дали копию документа?
Он знал, что мы достаточно опытны, чтобы сделать эту работу.
Предполагается, что новый конвейер введут в эксплуатацию на следующей неделе.
Топ-менеджер приказал закончить работу до 4 часов вечера.
Я предполагаю, что контракт будет подписан в ближайшем будущем.
Кто разрешил разгрузить товар? - Один из ваших менеджеров приказал разгрузить судно и отправить товар в город.
Говорят, что этот переводчик очень хорошо знает китайский. Он первоклассный специалист.

Задание 5. Расставьте знаки препинания в следующих предложениях:
Come and see me if you are ever in London
It is quite natural that you should want to meet your father
His wife was a tall elegant woman
It's a nice idea but there are a lot of if's he answered
I lent him The Old Man and the Sea which is really easy to read
He was the first man to swim the Bosporus I believe
I'd like to congratulate them but I don't know when I'll see them again
If I get a job I'll be able to pay off my debts

Контрольная работа
Темы 8-10. «Синтаксис. Пунктуация. Речевой этикет»

Вариант 2

Задание 1. Определите тип семантических отношений между элементами сложных предложений (координация, субординация, предикация).

The minute the door closed I felt alone. I felt so alone it was ridiculous.
What was certain was that I could not sleep again.
I understand all that but what I want to know is whether or not you have lost faith in me?

Задание 2. Подчеркните союзы, используемые для присоединения придаточных времени к главному предложению.

Mary looked at Tom, but he hardly ever talked when his mother was there.
He came in from the balcony just as she was screwing silver rings on to her ears.
I had a good look at the map while you were sleeping.
"Will you be long, Halt?" – "No, I'll be back as soon as I've finished briefing Andrwes."

Задание 3. Дополните следующие предложения, раскрыв скобки.
I wondered what… (to mean)
I understand they… (to come)
I don't see why … (to apologize)
You remember how … (to promise)
I know that… (to return)
I told him what … (to discuss)
I feel that … (to know)
I take it that …. (to be in the know).
I wish we … (to stay)
He suggested … (to have lunch).

Задание 4. Переведите следующие предложения на английский язык, используя the Complex Object and Complex Subject.
Сообщают, что товары на экспорт ожидают отправки (shipment) уже несколько дней.
Она разрешила отослать пробную партию товара в розничные магазины.
Я считаю, что этот человек очень опытный сотрудник.
Мы никогда не знали, что он ворует запасные части со склада.
Финансовый директор приказал сдать все отчеты до четверга.
Я предполагаю, что компания скоро обанкротится.
Объявили, что его назначили директором крупного завода.
Глава компании разрешил выдать зарплату рабочим.
Я прошу сообщить мне о любых изменениях в ваших планах.
Известно, что он придерживается другого мнения по этому вопросу.
Пунктуация

Задание 5. Расставьте знаки препинания в следующих предложениях:

She works for a company that organizes adventure holidays
Having made that decision we turned our attention to other matters
If you are ever in London come and see me
It looks rambling dirty and strange
Where is the book I bought yesterday
I believe he is the first man to swim the Bosporus
Quite honestly I think you should leave your job
It's nothing he gasped I'll be all right in a minute

Контрольная работа
Темы 1-2. «Карьера молодого специалиста. Медицина и здравоохранение»

Вариант 1

Задание 1. Напишите три формы неправильных глаголов:
to wear, to shake, to rise, to hold, to break, to quit, to mean, to win, to sell, to strive.

Задание 2. Переведите текст на английский язык, используя активную лексику.

Комната на чердаке. (The Skylight Room.)

(По рассказу О. Генри.)

Миссис Паркер - владелица меблированных комнат (furnished apartments) в одном из самых шумных и бедных районов Нью-Йорка. Когда очередной посетитель приходил к ней в поисках квартиры, она обычно показывала ему сначала самые дорогие комнаты. Поэтому посетители обычно отказывались, что неприятно удивляло хозяйку, и ей ничего не оставалось, как предложить посетителю самую дешевую комнату - комнату на чердаке.

Однажды в поисках комнаты здесь появилась молоденькая девушка, мисс Лисон (Leeson). У нее, как и у других посетителей м-с Паркер, не было намерения платить $12 в месяц за жилье (lodging). Она тоже могла позволить себе только комнату на чердаке.

Крохотная комнатушка, в которую служанка (maid) м-с Паркер проводила девушку, производила такое ужасное впечатление, что бедняжка в который раз пожалела, что у нее нет денег. Зато, подумала мисс Лисон, когда ночью в доме гасят свет, через окно в потолке, должно быть, видны звезды.

Самой яркой из этих звезд она даже дала имя - Уилли Джексон.

Осенью мисс Лисон уволили с работы, но это не вызвало сочувствия у м-с Паркер. Поэтому все деньги, которые удалось сэкономить, девушке приходилось отдавать за квартиру. Она голодала. Однажды ночью мисс Лисон почувствовала себя особенно плохо. Девушка посмотрела на небо и прошептала:

- Прощай, Уилли Джексон. Больше я тебя не увижу. Хотя, возможно, тебе уже надоело мое общество.

Утром служанка вызвала скорую. Молодому врачу, вынесшему мисс Лисон из комнаты на чердаке, было трудно сдержаться, чтобы не сказать м-с Паркер какую-нибудь резкость (to use sharp words to smb.).

На следующий день в газете появилась заметка об этом происшествии. Она заканчивалась словами: «Доктор Уильям Джексон, оказавший первую помощь (the ambulance doctor, who attended the case), утверждает, что больная выздоровеет».

Задание 3. Дайте развернутый ответ на следующий вопрос: Why is it not always easy for a beginning specialist to make a career.

Контрольная работа
Темы 1-2. «Карьера молодого специалиста. Медицина и здравоохранение»

Вариант 2

Задание 1. Напишите три формы неправильных глаголов:
to shine, to buy, to choose, sit, to pay, to cost, to fight, to beat, to fall, to keep.

Задание 2. Переведите текст на английский язык, используя активную лексику.

Последний лист.

(По рассказу О. Генри.)

Эта история произошла в пригороде Нью-Йорка, который в начале 20-го века был заселен (to be inhabited) бедными художниками и музыкантами. В одном из его домов снимали мастерскую (studio), одну на двоих (to share), две подруги; Сью (Sue) и Джонси (Johnsy). Джонси была такой маленькой и худенькой, что выглядела гораздо моложе своих лет.

Однажды осенью Джонси серьезно заболела воспалением легких. Встревоженная Сью решила показать подругу врачу. После осмотра доктор сказал. Сью, что сильно сомневается, удастся ли ему

вылечить Джонси. «Мне хорошо знаком этот случай, - сказал доктор, - Если бы Джонси хотела, она давно бы выздоровела. Но беда в том, что ей не хватает любви к жизни».

Когда Сью вернулась в комнату подруги, она увидела, что девушка пристально смотрит в окно и считает листья, облетающие со старого дерева, росшего во дворе у кирпичной стены. «Я жду, когда упадет последний лист, - прошептала Джонси, - Я умру вместе с ним. Я уже давно мечтаю покинуть этот мир».

Сью стоило больших усилий убедить подругу подремать. Когда Джонси наконец погрузилась в тяжелый сон, Сью вышла из комнаты и направилась к их соседу, старому художнику-неудачнику (unsuccessful artist) Берману (Behnnan), чтобы поделиться с ним своими переживаниями.

На следующее утро Сью увидела, что, несмотря на дождь и ветер, один лист все же остался на дереве. Удивительно, но он не упал ни на следующий день, ни через неделю, когда все деревья вокруг уже были голые.

Джонси выздоровела. Оказалось, что чудесный лист нарисовал на стене старик Берман. Он умер несколько дней спустя от пневмонии, которую подхватил, когда рисовал под дождем последний лист. Это был его единственный, но поистине гениальный шедевр (masterpiece).

Задание 3. Дайте развернутый ответ на следующий вопрос: A sound mind in a sound body.
Life’s not just being alive, but being well.
Health is better than wealth.

Keys
1. shine-shone-shone buy-bought-bought; choose-chose-chosen; sit-sat-sat; pay-paid-paid; cost-cost-cost; fight-fought-fought; beat-beat-beaten; fall-fell-fallen; keep-kept-kept;
2.
The Last Leaf.
This story happened in a suburb of New York, which at the beginning of the 20th century was inhabited by poor artists and musicians. Two girls, Sue and Johnsy, shared a studio in one of its houses. Johnsy was so small and thin that looked much less than her age.
One autumn Johnsy fell seriously ill with pneumonia. Sue decided to have her friend examined by a doctor. After the examination the doctor told Sue that he had grave doubts, if he would be able to cure Johnsy. 'The case is familiar to me, - the doctor said. - If Johnsy had wanted to recover, she would have recovered long ago. Bib the problem is that she is lacking in love for life.
When Sue returned to her friend's room, she saw that the girl was staring through the window and counting leaves falling from an old tree, which grew in the yard near a brick wall. cTm waiting for the last leaf to fail, - whispered Johnsy. -1 will die with it. I've been dreaming of leaving this world for a long time."
It was difficult for Sue to persuade her friend to doze a little. When at last Johnsy fell into a deep sleep, Sue left the room and went to their neighbor, an old unsuccessful artist Behrman, to share her sorrows with him.
Next morning Sue saw that, despite the rain and wind, one leaf remained on the tree. It was strange, but the leaf fell neither the following day, nor in a week, when ail trees around were naked.
Johnsy recovered. It turned out that old Behrman had painted the wonderful leaf on die brick wall. He died several days later of pneumonia, which he had caught when he was drawing the last leaf in the rain. It was his only masterpiece, but it v\ as a masterpiece of genius.

Контрольная работа
Темы 3-4. «Профессионализм, стрессовые ситуации на рабочем месте. Межличностное общение»
Вариант 1

Задание 1. Напишите три формы неправильных глаголов:
to find, to speed, to stroke, to lay, to drive, to lie, to laugh, to withdraw, to arise, to deal, to leave.
Задание 2. Переведите текст на английский язык, используя активную лексику.

Было семь часов, когда кофе варился, а сковородка была на плите, готовая для жарки котлет. Джим никогда не опаздывал. Делла завернула подарок и вернулась на свое место на краешке стола рядом с дверью, через которую он всегда входил в дом. Она сидела неподвижно, раздумывая, будут ли положительно приняты перемены в ее внешности. Когда она услышала его шаги на лестнице, она побледнела. Она была на грани паники, несмотря на то, что предприняла все меры предосторожности перед его приходом: при помощи щипцов для завивки она сделала себе на голове такие милые

кудряшки, что стала похожа на школьника-сорванца. Увидев себя в зеркале, она осталась довольна, но сейчас при звуке его шагов ее прежнее мужество куда-то испарилось.

Когда он дошел до последней ступеньки, ее нервы были уже на пределе. Дверь открылась, и вошел Джим.

Он выглядел очень худым и серьезным. Ему было только 22, а в его возрасте иметь дело с семейными проблемами было далеко не легкой задачей, особенно когда у тебя мало опыта в содержании семьи.

Как только Джим переступил порог, его взгляд застыл на Делле. Это был критический момент, поскольку она не могла прочесть выражение его глаз и это ее пугало. Это был не гнев, и не удивление, и не осуждение, и не ужас, и не одна из тех реакций, к которым она себя подготовила. Она кинулась к нему. «Джим, дорогой, - воскликнула она. - Не смотри на меня так. Я отрезала волосы и продала их, потому что не могу оставить тебя без подарка на Рождество! А теперь тебе лучше улыбнуться и пожелать мне счастливого праздника, потому что у меня для тебя есть изумительный подарок!» Джим внимательно оглядел комнату. У него был такой вид, будто он не понимал, к чему она клонит. Затем он пришел в себя, достал сверток из кармана пальто и швырнул его на стол. Это был подарок для нее. Делла восторженно вскрикнула и быстро разделалась с упаковкой и ленточкой. В тот же момент восторг сменился потоками слез. Подарок оказался ничем иным, как набором роскошных черепаховых гребней, который она вот уже, сколько месяцев вожделенно рассматривала в витрине Бродвейского магазина. Это был подарок, который превзошел все ожидания. Делла грустно улыбнулась и сказала: «У меня быстро растут волосы, Джим».

Задание 3. Дайте развернутый ответ на следующий вопрос: If you treat every situation as a life and death matter, you'll die a lot of times.

Контрольная работа
Темы 3-4. «Профессионализм, стрессовые ситуации на рабочем месте. Межличностное общение»
Вариант 2

Задание 1. Напишите три формы неправильных глаголов:
to rise, to fail, to pay, to cost, to beat, to mean, to win, to choose, to shine, to drive.

Задание 2. Переведите текст на английский язык, используя активную лексику.

.

Это история о человеке по имени Джордж Элефант. Он был обычным человеком и никогда не позволял себе причинять вред другим людям. Как это ни странно, но именно его имя сделало из него убийцу. Однажды он убил свою жену, пришел в полицейский участок, где во всем сознался. Все это было очевидным, и дело казалось простым, и все бы так и осталось, если бы не сэр Гордон Макинтош, знаменитый адвокат, который взялся за дело Элефанта. Мистер Макинтош был человеком чести и не мог позволить, чтобы его клиентов невинно осуждали. Поэтому он детально изучил дело, и ему предоставили факты о жизни и детстве Джорджа. Как оказалось, Джордж немного стыдился своей фамилии, никогда не чувствовал себя с ней удобно и даже хотел сменить ее. С самого детства Джордж страдал, так как люди находили большое удовольствие и развлечение, обзывая его различными именами животных, и очень ему тем самым досаждали. Он даже думал отказаться от телефона, чтобы оградить себя от ужасных шутников, но телефон был удобен и он оставил его. Его жена Джейн стала последней каплей в чаше его терпения. Джордж всегда думал, что супруги должны держаться вместе и делить невзгоды пополам, но это был не его случай. Джейн просто смеялась над ним из-за фамилии.

Таковы были факты, на которые опирался Макинтош в суде, и он был так уверен в победе, что даже хотел заключить пари. В конце концов, Элефанта не признали виновным в убийстве, но отправили на исправительные работы на 7 лет. Дело пробудило большой интерес у публики, и многие пораженные люди писали в газеты. Семь лет спустя, за неделю до выхода Элефанта из тюрьмы, туда приехал священник. Он хотел, чтобы заключенный исповедался и рассказал ему, что его тревожит, и таким образом несчастный вышел бы из тюрьмы полностью прощенным и со спокойной душой. Священник спросил Джорджа об убийстве и о его причине. «Честно говоря, - ответил Джордж. - Я был влюблен в другую женщину».

Задание 3. Дайте развернутый ответ на следующий вопрос::
Treat others as you would like them to treat you.

Контрольная работа
Тема 5. «Социальные проблемы. Судебное разбирательство»

Вариант 1

Задание 1. Напишите три формы неправильных глаголов:
to swear, to hit, to stick, to throw, to drink, to try, to run, to hurt, to flow, to bet.

Задание 2. Переведите текст на английский язык, используя активную лексику.

Семья Джексона жила в тяжелых условиях. Он был единственным человеком, который обеспечивал семью. Джексон был рабочим на местном заводе. На этом заводе часто происходили несчастные случаи. Людям приходилось работать сверхурочно.

Однажды Джексон попытался спасти оборудование от порчи, но повредил свою руку. Он не нарушал правил эксплуатации оборудования.

После того, как он вышел из больницы, Джексон уже не мог возвратиться к работе. Его положение было ужасным. Он был не в состоянии работать не этом заводе. Когда он попытался получить компенсацию, компания наняла высокопрофессиональных юристов и выиграла дело. Полковник Инграм был мастером в проведении перекрестного допроса, а показания свидетелей только помогли другой стороне. Но Джексон был ни в кой мере виновным. Право было на его стороне, но компания не уделяла никакого внимания его горю. Поскольку его здоровье сильно ухудшилось, и он не мог больше работать, он еле-еле сводил концы с концами и задолжал за квартиру.

Авис Канингам была потрясена историей Джексона. Она решительно настроилась расследовать это дело. Для неё самой это стало ужасным откровением. Она осознала, что с Джексоном поступили несправедливо. Она содрогалась при мысли о том, что цивилизация была основана на крови.

Авис нашла Джексона в ветхом доме недалеко от болота. Он был больше не в состоянии зарабатывать деньги, а у его жены было плохое здоровье. Джексон не рассказал ничего нового Авис, за исключением нескольких ужасных подробностей. После этого у неё был разговор с полковником Ингрэмом. Он признал, что Джексон должен был получить компенсацию после суда. Но на работе полковник Инграм руководствовался только профессиональными чувствами.

Все свидетели тряслись за свои собственные семьи и зависели от политики компании.

Никто не был в состоянии защитить Джексона. Никто не заботился о его будущем

Задание 3. Дайте развернутый ответ на следующий вопрос:
1) One law for the rich and another for the poor.
2) To no man will we sell, or deny, or delay, right or justice. (Magna Carta)

Контрольная работа
Тема 5. «Социальные проблемы. Судебное разбирательство»

Вариант 2

Задание 1. Напишите три формы неправильных глаголов:
to sink, to thank, to bet, to concern, to ruin, to despise, to throw, to hurt, to enjoy, to hold.

Задание 2. Переведите текст на английский язык, используя активную лексику.

Когда Том впервые приехал в школу, то очень удивился, увидев, каким великолепным и величественным было само здание. Он хотел бы больше знать о своих однокурсниках, т.к. очень хотел найти себе друзей. Его жизнь дома была ужасной. Отец с трудом сводил концы с концами, и был эгоистичным и жестоким человеком. Он никогда не жалел своего сына /не относился благожелательно к своему сыну.

Отец не хотел отправлять Тома в школу, потому что рассчитывал, что тот начнет работать, и они смогут скопить немного денег. Поэтому он удивился, узнав, что Том получил грант в престижной частной школе. Вначале он отнесся к этому приглашению как к шутке, но потом подумал, что это поможет ему избежать хлопот, и отпустил мальчика. Но провожать его на станцию так и не пошел.

Когда один из сотрудников школы проводил Тома в главный холл, тот очень нервничал. Но он постарался взять себя в руки, потому что хотел произвести хорошее впечатление на своих новых одноклассников.

В холле он увидел несколько мальчиков, примерно одного с ним возраста. Они подождали, пока он подойдет поближе. Затем один из них заметил что-то насчет потрепанной одежды Тома. Том не мог не услышать его слова. Он понял, что его несостоявшиеся друзья высмеивают его. Он был так неприятно поражен, что ему захотелось расплакаться, но он смог сохранить самообладание. Мальчишки ждали его ответа, он чувствовал на себе их внимательные взгляды. Ему захотелось сказать что-то умное и дерзкое (impertinent), но он так ничего и не сказал. Не было никакого смысла быть храбрым, не важно, что он скажет, они все равно будут относиться к нему как к изгою.

Задание 3. Дайте развернутый ответ на следующий вопрос:

1) One law for the rich and another for the poor.
2) To no man will we sell, or deny, or delay, right or justice. (Magna Carta)

Контрольная работа
Тема 6. «Личность и общество»
Вариант 1

Задание 1. Выберите правильный вариант:

He had changed so much since I last saw him that I could hardly .... him.
a) catch a glimpse of, b) distinguish, c) recognize
I only ...him, so I can't really say whether he was wearing a hat or not.
a)noticed, b) caught a glimpse of, c) glared
I waved to ... her attention, but she walked away without noticing me.
a)draw, b) attract, c) catch a glimpse of
I wanted to order coffee, but the waiter was so busy that it was very difficult to....
a) draw his attention, b) call his attention, c) catch his eye
She ... of me window for a moment, then carried on working.
a)caught a glimpse, b) glanced out, c) snatched a look

Задание 2. Переведите текст на английский язык, используя активную лексику.

Миссис Паклтайд (Mrs. Packletide) была амбициозной женщиной. Она завидовала миссис Луне Бимбертон (Mrs. Loona Bimberton), а её слава отравляла жизнь Миссис Паклтайд. Несмотря на это, она не имела намерения сдаваться. Она решила убить тигра и завладеть его шкурой. Мысль о том, что она добьется популярности, увлекла миссис Паклтайд.

Миссис Паклтайд сделала все приготовления для охоты. Она назначила дату для этого события и пригласила миссис Меббин (Mrs. Mebbin) в качестве компаньона, которой заплатила. Миссис Меббин очень хотела заполучить деньги и только об этом думала.

Способности к охоте Миссис Паклтайд оставляли желать лучшего. Поэтому, чтобы избежать особого риска и напряжения, она предприняла все меры предосторожности и попросила местных жителей сделать все приготовления для охоты. Козел послужил в качестве приманки. А ружьё было точно прицелено. Убить тигра не было большим риском, поскольку он был уже старым и больным.

В назначенное время две охотницы поджидали, когда появится их жертва. Миссис Паклтайд уже мечтала, как она будет давать обед в честь Луны Бимбертон, когда её размышления были прерваны появлением самого тигра. Она чуть было не вскрикнула от страха, но сдержалась. Последовал громкий выстрел ружья. Зверь упал и умер. Миссис Паклтайд облегченно вздохнула. Но миссис Меббин заметила рану на теле козла. Короче говоря, он поняла, что козел был убит, а тигр умер от остановки сердца.

Миссис Меббин обратила внимание миссис Паклтайд на то, что не то животное было убито. Миссис Паклтайд была раздосадована. Она побледнела, но не дала выхода своим чувствам. Миссис Паклтайд содрогнулась при мысли о том, что её могли разоблачить. Она попросила миссис Меббин не выдавать её. Но Миссис Меббин была себе на уме и увидела в этом возможность потребовать от Миссис Паклтайд ещё денег. Миссис Паклтайд пожалела о том, что доверилась миссис Меббин и уже собиралась высказать ей всё, что она о ней думала, но сдержалась.

Таким образом, слава о Миссис Паклтайд распространилась повсюду. Условия миссис Меббин были выполнены, она получила деньги и купила хороший загородный домик.

Задание 3. Дайте развернутый ответ на следующий вопрос:

Beware, as long as you live, of judging people by appearances. (J.de la Fontaine)

Characters never change. Opinions alter, - characters are only developed.(B. Disraeli)
Beauty is everywhere a welcome guest. (J. W. von Goethe)
Talkers are no good doers.(W. Shakespeare)

Контрольная работа
Тема 6. «Личность и общество»
Вариант 2

Задание 1. Выберите правильный вариант:

She wanted to order ice-cream but the waiter was so busy that it was very difficult to....
a) draw his attention, b) call his attention, c) catch his eye
Ann ... of the window for a moment then carried on writing.
a)caught a glimpse, b) glanced out, c) snatched a look
Mike had changed so much since we last met that I could hardly .... him.
a) catch a glimpse of, b) distinguish, c) recognize
We only ...him, so I can't really say whether he was wearing a hat or not.
a) noticed, b) caught a glimpse of, c) glared
He waved to ... their attention, but they walked away without noticing him.
a) draw, b) attract, c) catch a glimpse of

Задание 2. Переведите текст на английский язык, используя активную лексику.

Было четыре часа утра, но Кемп все еще работал. Он любил работать ночью, когда его никто не беспокоил. Он чувствовал себя усталым, так как работал с раннего утра. Кемп решил лечь спать и вошел в спальню. Молодой человек удивился, увидев, что его постель в беспорядке. Некоторое время он стоял не двигаясь, он вспомнил все разговоры о Невидимке. И, хотя, он не верил в эти истории, он чувствовал себя неловко. Кемп пожалел, что не закрыл дверь на ключ. Ему даже показалось, что на него пристально смотрят. "Неужели я все это придумываю, " - подумал Кемп. "Мне нужно избавиться от этой привычки работать по ночам."

Вдруг Кемп услышал, как чей-то голос сказал: "О боже, это никто иной, как Кемп!" И снова была тишина, только кто-то глубоко вздохнул. Когда кто-то дотронулся до его плеча, от этого у него упало сердце, и его охватил ужас. Но тот же самый голос пытался успокоить его: "Кемп, не нервничай, это я, Гриффин. Мы учились с тобой в университете 6 лет назад. Уже в течение нескольких лет я работаю над проблемой невидимости и должно быть я добился успехов, так как я сейчас невидим." Кемп едва себя сдерживал. Его лицо выражало ужас. Ему нелегко было взять себя в руки. Но вдруг его внимание привлек бинт, висящий в воздухе.

"Ты ранен?" - спросил Кемп, дрожа от волнения.

"Ради бога, Кемп, дай мне что-нибудь поесть. Я едва на ногах держусь от голода и усталости. Я не спал уже несколько дней" - прошептал Гриффин слабым голосом. "Как ты стал невидимым?" "Веришь ли ты, что я гениальный ученый? У меня великолепные идеи, но мне нужны деньги. Если бы ты только мог мне помочь! Если бы у меня был талантливый ассистент, я бы стал хозяином мира. Теперь, когда я нашел тебя, мы сотворим чудеса!"

Кемп пригласил Гриффина присесть, принес ему еды и предложил, что бы он остался у него на ночь. Он включил свет так, чтобы никто ничего не заметил с улицы.

"Я думал, что все это выдумка," - сказал Кемп, откашлявшись. "Если бы я не встретил тебя дома, я никогда бы не поверил, что Невидимка существует на самом деле. Расскажи мне все подробно, верь, что желанный гость в моем доме, и ты можешь мне доверять."

Задание 3. Дайте развернутый ответ на следующий вопрос:

Beware, as long as you live, of judging people by appearances. (J.de la Fontaine)
Characters never change. Opinions alter, - characters are only developed.(B. Disraeli)
Beauty is everywhere a welcome guest. (J. W. von Goethe)
Talkers are no good doers.(W. Shakespeare)

Контрольная работа
Тема 7. «Власть и политика»
Вариант 1

Задание 1. Переведите текст на английский язык, используя активную лексику.

Основной целью визита американского президента во Вьетнам было, восстановление дипломатических отношений между двумя странами. При ЭТОМ накануне исторического визита,

который был назначен на ноябрь 2000, президент Клинтон дал понять, что не намеревается приносить официальные извинения за ущерб, причиненный Вьетнаму.

Молодые вьетнамцы оказали ' президенту США радушный прием: толпы молодежи собирались на улицах, чтобы хоть мельком взглянуть на него. Однако визит главы сверх державы вызвал крайнее раздражение и недовольство старшего поколения, которое не в состоянии забыть пережитое горе. Многие из них содрогнулись при * мысли, что вновь увидят флаг бывшего врага на своей территории. Зарубежные журналисты посетили старую вьетнамку, потерявшую на войне мужа и шестерых сыновей. Она не сдерживала своих эмоций, и гостям было трудно смотреть ей в глаза, поэтому они предпочли сократить свой визит.

Президент США путешествовал повсюду, но никогда ранее не бывал в этой маленькой стране, нанесшей Америке унизительное поражение в войне. Накануне визита у президента были сомнения, правильно ли выбран момент для посещения Вьетнама. Он не хотел рисковать и потерпеть еще и дипломатическое поражение. Но у президента было преимущество: он лично не испытывал чувства вины, так как в свое время уклонился от призыва (to avoid the draft) и не воевал во Вьетнаме.

Задание 2. Суммируйте содержание текста

THE SECOND WORLD WAR

The people of Britain watched anxiously as German control spread over Europe in the 1930s. In September 1939 Germany invaded Poland, and Britain entered the war. The British felt again that they were fighting for the weaker nations of Europe, and for democracy. They had also heard about the cruelty of the Nazis from Jews who had escaped to Britain.

Few people realised how strong the German army was. In May 1940 it attacked, defeating the French in a few days, and driving the British army into the sea. At Dunkirk, a small French port, the British army was saved by thousands of private boats which crossed the English Channel. Dunkirk was a miraculous rescue from military disaster, and Britain's new Prime Minister, Winston Churchill persuaded the nation that it was a victory of courage and determination at Britain's darkest hour. Although the army had lost almost all its weapons in France, Churchill cold the nation there could be no thought of surrender or peace negotiation: "we shall defend our island, whatever the cost may be, we shall fight on the beaches, we shall fight on the landing grounds, we shall tight in the fields and in the streets, we shall right on the hills; we shall never surrender. ... until in God's good time the New World, with all its power and might, sets forth to the liberation and rescue of the Old." And he offered his countrymen nothing but "blood, toil, tears and sweat."

Everyone in Britain expected Germany to invade, but the British air force won an important battle against German planes in the air over Britain. This, however, did not prevent the German air force from bombing the towns of Britain. Almost one and a half million people in London were made homeless by German bombing during the next few months. Once again Churchill brilliantly managed to persuade n nation "on its knees" that it would still win.

The war had begun as a traditional European struggle, with Britain fighting to save the "balance of power" in Europe, and to control the Atlantic Ocean and the sea surrounding Britain. But the war quickly became worldwide. Both sides wanted to control the oil in the Middle East, and the Suez Canal, Britain's route to India. In 1941 Japan, Germany's ally, attacked British colonial possessions, including Malaya (Malaysia), Burma and India. As a result, Britain used soldiers from all parts of its empire to help fight against Germany, Italy and Japan. But the weakness of Britain was obvious to the whole world when its army surrendered Singapore to Japan, described by Churchill as the worst surrender in British history.

David McDowall
History of Britain

Контрольная работа
Тема 7. «Власть и политика»
Вариант 2

Задание 1. Переведите текст на английский язык, используя активную лексику.

У Тэкера было такое чувство, что его ловко провели. Ему ужасно хотелось высказать Киду все, что он думает о нем, но, поразмыслив немного, понял, что при таком положении дел, он не может позволить себе такой роскоши. Всю ночь Тэкер не спал. У него был измученный вид. При одной только мысли, что его может схватить полиция, он чувствовал себя ужасно. Если бы не этот Кид, я бы уже давно отсюда уехал". Тэкер больше не мог сдерживаться. От Кида не было известий, и Тэкер потерял

всякую надежду прояснить ситуацию. Но он решил не поддаваться отчаянию, и сам отправился в особняк дона Uriques. Кид был явно раздражен, когда заметил Тэкера.

- Не надо было вам приходить сюда! Вы бы сэкономили себе массу времени и нервов.

- Полностью разделяю твое мнение. Но я хотел удостовериться, что ты не передумал… Не следует тебе, Кид, задирать нос передо мной. Ты дал мне понять, что через неделю ты украдешь деньги, мы разделим их на две равные части, а прошло уже две. Это становится невыносимым. Что помешало тебе вскрыть сейф? Почему ты не воспользовался такой возможностью?

Тэкер замолчал, чтобы перевести дыхание, он с трудом пытался найти слова. Он был охвачен гневом. Кид смотрел на него, не отводя глаз.

- Многое изменилось за эти короткие две недели. Вы же помните, через что пришлось пройти моей бедной матери. Она была охвачена горем, когда меня похитили много лет назад. Теперь моя очередь делить с ней все тревоги и волнения. И, если, я уйду опять, она умрет от разрыва сердца.

Тэкер прервал Кида.

- Это смешно! Неужели ты думаешь, что твоя история тронет меня до глубины души! Зачем только я посвятил тебя в свой план! Он был гениальным, совершенно безопасным. Ты ничем не рисковал. Ты сам говорил, что примешь столь заманчивое предложение. Моему терпению настал конец. Я выдам тебя!

- Во всяком случае, если бы меня застали на месте преступления, я бы сделал все возможное, чтобы обвинить вас. Вы сами попустительствовали тому, что я появился в доме дона Uriques в качестве их потерянного сына. Не забывайте также о моем прошлом. Всю свою жизнь я был предоставлен сам себе. Поэтому я привык делать все сам, поступать по-своему.. К тому же, я отменно стреляю. Короче говоря, я решил начать жизнь с нового листа. И если вы встанете у меня на пути, вы очень рискуете погубить свою жизнь, не говоря уже о карьере. Запомните, мои поступки продиктованы не столько ненавистью к вам, сколько жалостью и любовью к моей вновь обретенной матери. Даю вам последнее предупреждение(warning).

Тэкер был глубоко уязвлен. Его охватил страх, он не мог пошевельнуться. Он понял, что проиграл.

Задание 2. Суммируйте содержание текста

THE SECOND WORLD WAR

In 1941 Germany and Japan had made two mistakes which undoubtedly cost them the war. Germany attacked the Soviet Union, and Japan attacked the United States, both quite unexpectedly. Whatever the advantages of surprise attack, the Axis of Germany, Italy and Japan had now forced onto the battlefield two of the most powerful nations in the world.

Britain could not possibly have defeated Germany without the help of its stronger allies, the Soviet Union and the United States. By 1943 the Soviet army was pushing the Germans out of the USSR, and Britain had driven German and Italian troops out of North Africa. Italy surrendered quickly following Allied landings in July 1943. In 1944 Britain and the United States invaded German-occupied France. They had already started to bob German towns, causing greater destruction than any war had ever caused before. Such bombing had very doubtful military results. Dresden, a particularly beautiful eighteenth-century city, and most of its 130,000 inhabitants, were destroyed in one night early in 1945. In May 1945, Germany finally surrendered. In order to save further casualties among their own troops, Britain and the United States then used their bombing power to defeat Japan. This time they used the new atomic bombs to destroy most of Nagasaki and Hiroshima, two large Japanese cities. Over 110,000 people died immediately and many thousands more died later from the after-effects.

It was a terrible end to the war, and an equally terrible beginning to the post-war world. But at the time there was great relief in Britain that the war had finally ended. It had lasted longer than the First World War, and although less than half as many British troops had died this time, the figures of over 303,000 soldiers and 60,000 civilians in air raids was a very heavy price to pay for the mistakes of the inter-war years. The Soviet Union, Germany and Japan paid a fair more terrible price, as did ethnic groups like the Jewish and gypsy peoples, several million of whom were deliberately killed.

David McDowall
History of Britain

Контрольная работа
3 курс 5 семестр

Темы 8-10. Информация как основной элемент системы безопасности. История создания информационной безопасности. Информационная безопасность

Задание 1. Кратко сформулируйте основную идею текста

News is happening all the time: People are being born or dying, banks are being robbed, roads are being planned, companies are making profits or losses, storms are destroying homes, courts are sending people to jail or freeing them, scientists are discovering new drugs. Every minute of every day something newsworthy is happening somewhere in the world.

Even if you are a journalist working in a small country, something newsworthy is probably happening in your country at this moment, while you are reading this book. Your job as a journalist is to get information on those events and present it to your readers or listeners. But you cannot be everywhere all the time to see those events for yourself. So you need other ways of getting information on all those hundreds (maybe millions) of events you cannot witness yourself. When someone or something provides you with information, we call them a source.

Sources of information can be people, letters, books, files, films, tapes - in fact, anything which journalists use to put news stories together. Sources are very important if you want to report on events or issues and explain the world to your audience. Journalists try to work as much as possible from their own observations, but this is often not possible. Some events or issues are finished before the journalist gets there. Others are like plants which only show their stem and leaves above the ground - the all-important roots are hidden from sight. Journalists who only report what they see can miss much of the news unless they have sources to tell them of more details or other aspects which are out of sight.

Journalists should deal in reliable facts, so it is important that the sources you use for writing stories can give you accurate information about what happened or what was said. But just as there are lots of different news events, so there are many different sources of information. Some of them will give you very accurate information and we call these sources reliable (because we can rely on what they say). Others are less reliable, but still useful, while some can hardly be trusted at all. The main way of judging sources of information is on their reliability.

Задание 2. Ссоставьте план текста

Mobile device use in colleges and universities allows flexibility in access and working arrangements for staff and is actively encouraged.

Areas of use include:

Learning activities on fieldtrips and work placements and ongoing professional training

Information provision – assessments, feedback, lecture time changes, pastoral appointments

Information gathering for research purposes – eg recording of face-to-face interviews

Staff copying central service files to work on at home or note taking in an external meeting

All of the activities listed above may lead to inadvertent or deliberate processing of personal information often for reasons of convenience or ease of use. They also raise issues of consent and confidentiality.

Many mobile devices have the capability of copying and storing information accessed via a secure password protected network. They offer flexibility of access to information and learning at convenient times and offer control of pace. They can also aid more relevant and timely feedback from tutors. On the downside, this flexibility may place added pressures on employees which may in turn lead to unauthorised disclosure of personal or confidential data.

The Data Protection Act 1998 (DPA) places certain obligations upon organisations prior to, and during, their use of personal data and it grants individuals certain rights regarding the personal information held about them by organisations. The DPA covers ‘personal data’ and ‘sensitive personal data’. ‘Personal data’ is any information about an identifiable living individual regardless of the format of information.

This does not mean every document which has the data subject’s name on it will be personal data, but the overriding test is whether the information in question affects a

person’s privacy, or in other words, whether it is significant biographical information. ‘Sensitive personal data’ comprises information including an individual’s race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions.

It should be noted here that the DPA does not apply to confidential information which does not contain personal data. This data may still require enhanced security but its processing is not regulated by the DPA. Examples are research and unpublished academic work which may have the potential for patent application or draft financial plans to reduce departmental costs.

The DPA doesn't distinguish between data on-site and data taken off-campus, and the obligations on the data controller (ie the college or university) to ensure appropriate security remain the same, but the challenges in controlling and securing the data increase. The data user's requirements and expectations on ease of handling and mobility are also increasing with developments in technology, as are the pressures placed on staff to be able to work anytime anywhere.

Задание 3. Суммируйте содержание текста

The numerous technical advances in information sciences do not always produce more secure environments. Therefore, information security cannot be understood or described as solely a technical problem. Computers are operated by people and this means that information security is also a human factors issue. Human factors influence how individuals interact with information security technology; it is this interaction that is often detrimental to security.

It is evident that solely technical solutions are unlikely to prevent security breaches. Organisations need to instil and maintain a culture where positive security behaviours are valued. The usability challenges associated with information security need to be understood and resolved. This means that security functions need to be meaningful, easy to locate, visible and convenient to use. Employees need to be educated about the importance of security awareness, and this should incorporate behavioural training.

How individuals interact with computers and how decisions are made in regard to information security is certainly a very dynamic and complex issue. There are many factors that need to be considered. For example, it is important to acknowledge the influence of individual differences, personality traits and cognitive abilities. There are also biases and heuristics that affect how individuals perceive risk. These are important because they help to explain why individuals make certain decisions and why specific behaviours may be observed.

Both risk perception and individual differences are also affected by the environment in which they occur. Culture and climate can certainly have a significant impact on values, attitudes and behaviours. That is why understanding an organisation's culture and security climate can provide great insights into why certain behaviours do and do not take place.

A major concern within information security is the threat of social engineering attacks. Social engineering attacks are conducted in an effort to gain sensitive information, and this information is often used maliciously to the detriment of individuals and organisations. Social engineering poses a real threat to all organisations and to diminish this threat, individuals need to not only be aware of potential attacks, but also taught the appropriate tools to reduce their chances of becoming a target and a victim.

Задание 4. Изложите содержание текста на английском языке используя активную лексику.

Основы обеспечения информационной безопасности организации

Конфиденциальная для бизнеса информация входит в сферу повышенного интереса конкурирующих компаний. Для недобросовестных конкурентов, коррупционеров и других злоумышленников особый интерес представляет информация о составе менеджмента предприятий, их статусе и деятельности фирмы. Доступ к конфиденциальной информации и ее изменение могут нанести существенный урон финансовому положению компании. При этом, информационная утечка может быть даже частичной. В некоторых случаях даже обеспечение хищения 1/5 конфиденциальной информации может иметь

критические последствия для финансовой безопасности. Причиной утечки информации, если отсутствует должное обеспечение информационной безопасности организации, могут быть различные случайности, вызванные неопытностью сотрудников.

Информационная безопасность предполагает обеспечение защиты данных от хищений или изменений как случайного, так и умышленного характера. Система обеспечения информационной безопасности организации – эффективный инструмент защиты интересов собственников и пользователей информации. Следует отметить, что ущерб может быть нанесен не только несанкционированным доступом к информации. Он может быть получен в результате поломки коммуникационного или информационного оборудования. Особенно актуальна эффективная организация обеспечения безопасности информационных банковских систем и учреждений открытого типа (учебные, социальные и др.).

Для того чтобы наладить должное обеспечение защиты информации следует иметь четкое представление об основных понятиях, целях и роли информационной безопасности.

Термин «безопасность информации» описывает ситуацию, исключающую доступ для просмотра, модерации и уничтожения данных субъектами без наличия соответствующих прав. Это

понятие включает обеспечение защиты от утечки и кражи информации с помощью современных технологий и инновационных устройств.

Защита информации включает полный комплекс мер по обеспечении целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права.

Целостность – понятие, определяющее сохранность качества информации и ее свойств.

Конфиденциальность предполагает обеспечение секретности данных и доступа к определенной информации отдельным пользователям.

Доступность – качество информации, определяющее ее быстрое и точное

нахождение конкретными пользователями.

Цель защиты информации – минимизация ущерба вследствие нарушения требований целостности, конфиденциальности и доступности.

Система безопасности обеспечивается работой таких подразделений, как:

Компьютерная безопасность. Работа этого подразделения основана на принятии технологических и административных мер, которые обеспечивают качественную работу всех аппаратных компьютерных систем, что позволяет создать единый, целостный, доступный и конфиденциальный ресурс.

Безопасность данных - это защита информации от халатных, случайных, неавторизированных или умышленных разглашений данных или взлома системы.

Безопасное программное обеспечение - это целый комплекс прикладных и общецелевых программных средств, направленных на обеспечение безопасной работы всех систем и безопасную обработку данных.

Безопасность коммуникаций обеспечивается за счет аутентификации систем телекоммуникаций, предотвращающих доступность информации неавторизированным лицам, которая может быть выдана на телекоммуникационный запрос. http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/

Задание 5. Дайте определения основным понятиям из области информационной безопасности.

Задание 6. Прокомментируйте следующее высказывание:

"In the last 20 years, technology has permeated every facet of the business environment. The business place is no longer static – it moves whenever employees travel from office to office, from office to home, from city to city. Since business has become more fluid, information security is no longer the sole responsibility of a small dedicated group of professionals ….."

Контрольная работа
3 курс 5 семестр
Темы 11-16. Организационная структура предприятия с точки зрения информационной безопасности. Система принятия решений в организации. Управление корпоративным информационным контентом. Этика в информационной безопасности. Система управления качеством. Модели информационной безопасности на предприятии.

Задание 1. Кратко сформулируйте основную идею текста

Typically, a security policy has a hierarchical pattern. It means that inferior staff is usually bound not to share the little amount of information they have unless explicitly authorized. Conversely, a senior manager may have enough authority to make a decision what data can be shared and with whom, which means that they are not tied down by the same information security policy terms. So the logic demands that ISP should address every basic position in the organization with specifications that will clarify their authoritative status.

Policy refinement takes place simultaneously with defining the administrative control, or authority in other words, people in the organization have. In essence, it is hierarchy-based delegation of control in which one may have authority over his own work, project manager has authority over project files belonging to a group he is appointed to, and the system administrator has authority solely over system files – a structure reminiscent of the separation of powers doctrine. Obviously, a user may have the "need-to-know" for a particular type of information. Therefore, data must have enough granularity attribute in order to allow the appropriate authorized access. This is the thin line of finding the delicate balance between permitting access to those who need to use the data as part of their job and denying such to unauthorized entities.

Access to company's network and servers, whether or not in the physical sense of the word, should be via unique logins that require authentication in the form of either passwords, biometrics, ID cards, or tokens etc. Monitoring on all systems must be implemented to record logon attempts (both successful ones and failures) and exact date and time of logon and logoff.

Speaking of evolution in the previous point – as the IT security program matures, the policy may need updating. While doing so will not necessarily be tantamount to improvement in security, it is nevertheless a sensible recommendation.

Задание 2. Составьте план текста

Data can have different value. Gradations in the value index may impose separation and specific handling regimes/procedures for each kind. An information classification system therefore may succeed to pay attention to protection of data that has significant importance for the organization, and leave out insignificant information that would otherwise overburden organization's resources. Data classification policy may arrange the entire set of information as follows:

High Risk Class– data protected by state and federal legislation (the Data Protection Act, HIPAA, FERPA) as well as financial, payroll, and personnel (privacy requirements) are included here.

Confidential Class – the data in this class does not enjoy the privilege of being under the wing of law, but the data owner judges that it should be protected against unauthorized disclosure.

Class Public – This information can be freely distributed.

Data owners should determine both the data classification and the exact measures a data custodian needs to take to preserve the integrity in accordance to that level.

Sharing IT security policies with staff is a critical step. Making them read and sign to acknowledge a document does not necessarily mean that they are familiar with and understand the new policies. A training session would engage employees in positive attitude to information security, which will ensure that they get a notion of the procedures and mechanisms in place to protect the data, for instance, levels of confidentiality and data sensitivity issues. Such an awareness training should touch on a broad scope of vital topics: how to collect/use/delete data, maintain data quality, records management, confidentiality, privacy, appropriate utilization of IT systems, correct usage social networking, etc. A small test at the end is perhaps a good idea.

General considerations in this direction lean towards responsibility of persons appointed to carry out the implementation, education, incident response, user access reviews, and periodic updates of an ISP.

Prevention of theft, information know-how and industrial secrets that could benefit competitors are among the most cited reasons why a business may want to employ an ISP to defend its digital assets and intellectual rights.

Out of carelessness mostly, many organizations without giving a much thought choose to download IT policy samples from a website and copy/paste this ready-made material in attempt to readjust somehow their objectives and policy goals to a mould that is usually crude and has too broad-spectrum protection. Understandably, if the fit is not a quite right, the dress would eventually slip off.

A high-grade ISP can make the difference between growing business and successful one. Improved efficiency, increased productivity, clarity of the objectives each entity has, understanding what IT and data should be secured and why, identifying the type and levels of security required and defining the applicable information security best practices are enough reasons to back up this statement. To put a period to this topic in simple terms, let's say that if you want to lead a prosperous company in today's digital era, you certainly need to have a good information security policy.

http://resources.infosecinstitute.com/key-elements-information-security-policy/

Задание 3. Суммируйте содержание текста

Another caveat for the security professional using the sub-policy approach is to make sure sub-policies do not repeat what is in the global policy, and at the same time are consistent with it. Repetition must be prohibited as it would allow policy documents to get out of sync as they individually evolve. Rather, the sub-documents should refer back to the global document and the two documents should be linked in a manner convenient for the reader.

Even while giving sub-policies due respect, wherever there is an information security directive that can be interpreted in multiple ways without jeopardizing the organization's commitment to information security goals, a security professional should hesitate to include it in any policy. Policy should be reserved for mandates. Alternative implementation strategies can be stated as a responsibility, standard, process, procedure, or guideline. This allows for innovation and flexibility at the department level while still maintaining firm security objectives at the policy level.

This does not mean that the associated information protection goals should be removed from the information security program. It just means that not all security strategy can be documented at the policy level of executive mandate. As the information security program matures, the policy can be updated, but policy updates should not be necessary to gain incremental improvements in security. Additional consensus may be continuously improved using other types of Information Security Program documents.

Supplementary documents to consider are:

Roles and responsibilities — Descriptions of security responsibilities executed by departments other than the security group. For example, technology development departments may be tasked with testing for security vulnerabilities prior to deploying code and human resources departments may be tasked with keeping accurate lists of current employees and contractors.

Technology standards — Descriptions of technical configuration parameters and associated values that have been determined to ensure that management can control access to electronic information assets.

Process - Workflows demonstrating how security functions performed by different departments combine to ensure secure information-handling.

Procedures — Step by step instructions for untrained staff to perform routine security tasks in ways that ensure that the associated preventive, detective, and/or response mechanisms work as planned.

Guidelines — Advice on the easiest way to comply with security policy, usually written for non-technical users who have multiple options for secure information-handling processes.

What an information security policy includes

This leaves the question: what is the minimum information required to be included in an information security policy? It must be at least enough to communicate management aims and

direction with respect to security. It should include:

Scope — should address all information, systems, facilities, programs, data, networks and all users of technology in the organization, without exception

Information classification — should provide content-specific definitions rather than generic "confidential" or "restricted"

Management goals — goals for secure handling of information in each classification category (e.g., legal, regulatory, and contractual obligations for security) may be combined and phrased as generic objectives such as "customer privacy entails no authorized cleartext access to customer data for anyone but customer representatives and only for purposes of communicating with customer," "information integrity entails no write access outside accountable job functions," and "prevent loss of assets"

Context — Placement of the policy in the context of other management directives and supplementary documents (e.g., is agreed by all at executive level, all other information handling documents must be consistent with it)

Supporting documents — include references to supporting documents (e.g., roles and responsibilities, process, technology standards, procedures, guidelines)

Specific instructions — include instruction on well-established organization-wide security mandates (e.g., all access to any computer system requires identity verification and authentication, no sharing of individual authentication mechanisms)

Responsibilities — outline specific designation of well-established responsibilities (e.g., the technology department is the sole provider of telecommunications lines)

Consequences — include consequences for non-compliance (e.g., up to and including dismissal or termination of contract)

This list of items will suffice for information security policy completeness with respect to current industry best practice as long as accountability for prescribing specific security measures is established within the "supplementary documents" and "responsibilities" section. While items 6 and 7 may contain a large variety of other agreed-upon details with respect to security measures, it is ok to keep them to a minimum to maintain policy readability and rely on sub-policies or supporting documents to include the requirements. Again, it is more important to have complete compliance at the policy level than to have the policy include a lot of detail.

Note that the policy production process itself is something that necessarily exists outside of the policy document. Documentation with respect to policy approvals, updates and version control should also be carefully preserved and available in the event that the policy production process is audited.

https://www.csoonline.com/article/2124114/it-strategy/strategic-planning-erm-how-to-write-an-information-security-policy.html?page=2

Задание 4. Изложите содержание текста на английском языке используя активную лексику.

Безопасность информации предполагает отсутствие недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на ресурсы, используемые в автоматизированной системе. Критериями информационной безопасности являются конфиденциальность, целостность и будущая доступность информации. При этом под конфиденциальностью понимается свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц. Целостность -это свойство информационных ресурсов, в том числе информации, определяющее их точность и полноту. В свою очередь доступность информации - это свойство, определяющее возможность получения и использования информации по требованию уполномоченных лиц.

Следует подчеркнуть, что темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы, руководящих документов, действующих на территории России. Поэтому решение вопроса о разработке эффективной политики информационной безопасности на современном предприятии напрямую связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации.

Современные методы управления рисками позволяют решить ряд задач перспективного стратегического развития предприятия. Во-первых, количественно оценить текущий уровень информационной безопасности предприятия, что потребует выявления рисков на правовом, организационно-управленческом, технологическом и техническом уровнях обеспечения защиты информации. Во-вторых, в систему риск-менеджмента на предприятии может быть включена политика безопасности и планы совершенствования корпоративной системы защиты информации для достижения приемлемого уровня защищенности информационных активов компании.

С этой целью рекомендуется осуществить расчет финансовых вложений в обеспечение безопасности на основе технологий анализа рисков, произвести соотношение расходов на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения. Необходимо выявлять и проводить первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы. Следует определить функциональные отношения и зоны ответственности при взаимодействии подразделений и

лиц по обеспечению информационной безопасности предприятия, а также разработать необходимый пакет организационно-распорядительной документации. Одновременно следует осуществлять разработку и согласование со службами предприятия, надзорными органами проекта внедрения необходимого комплекса защиты, учитывающего современный уровень и тенденции развития информационных технологий. Кроме того, важным мероприятием поддержки системы безопасности информации является обеспечение поддержания внедренного комплекса защиты в соответствии с изменяющимися условиями работы предприятия, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Система защиты информации на предприятии преследует такие цели как предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Помимо этого система информационной безопасности нацелена на обеспечение устойчивого функционирования объекта: предотвращение угроз его безопасности, защиту законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом.

Обязательным условием эффективной реализации вышеупомянутых целей является непременный контроль качества предоставляемых услуг и обеспечение гарантий безопасности имущественных прав и интересов клиентов.

В связи с этим, система информационной безопасности должна базироваться на следующих принципах:

- прогнозирование и своевременное выявление угроз безопасности информационных ресурсов, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

- создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;

- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;

- создание условий для максимально возможного возмещения илокализации ущерба,

наносимого неправомерными действиями физических и юридических лиц и, тем самым, ослабление возможного негативного влияния последствий нарушения информационной безопасности.

При разработке политики безопасности рекомендуется использовать модель, основанную на адаптации общих критериев (ISO 15408) и проведении анализа риска (ISO 17799). Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарт)' ISO/IEC 15408 «Информационная технология - методы защиты - критерии оценки информационной безопасности», стандарту ISO/IEC 17799 «Управление информационной безопасностью».

Данная модель включает следующие объективные факторы:

- угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;

- уязвимости информационной системы или системы контрмер, влияющие на вероятность реализации угрозы;

- риск - фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования.

Предлагаемая методика разработки политики информационной безопасности современного предприятия позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходы на дополнительные меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

http://www.globez.ru/press/148-.html

Задание 5. Дайте определения основным понятиям из области информацинnной безопасности.

Задание 6. Прокомментируйте следующее высказывание: A company’s information is only as secure as its weakest link.

Контрольная работа
3 курс 6 семестр

Темы 17-20. Информация как актив предприятия. Информационные системы. Современные технологии и информационная безопасность. Жизненный цикл системы безопасности.

Задание 1. Кратко сформулируйте основную идею текста

IT-reliant work systems . The fact that a work system uses IT extensively does not imply that it is an information system. The following are examples of work systems that use IT extensively but are not information systems: fulfillment systems for phy package delivery systems, highly automated manufacturing systems, medical systems that include physical examination or treatment of patients, and transportation systems that use IT extensively. In such cases, an information system may produce inter mediate products and services that are meaningful and useful primarily in the context of a larger work system that involves activities beyond processing of information. Alternative ly, the processing of information may be so intertwined with the work system that it is barely meaningful to speak of the information system as a separate system.

Increasing reliance on computerized information systems has led to increasing degrees of overlap between work systems and the information systems that support them. This trend implies that a clear IS definition should distinguish between information systems and IT-reliant work systems (of which information systems are a special case whose processes and activities are devoted to information and that produce informational products and services). This distinction is often

ignored because IT-reliant work systems are sometimes treated as subject matter within in the IS field, an inclusion that may have significant benefits for the IS field. (Alter, 2003a; 2003b)

http://repository.usfca.edu/cgi/viewcontent.cgi?article=1021&context=at

Задание 2. Составьте план текста

Ransomware refers to a type of malware used by attackers that first encrypts files and then attempts to extort money in return for the key to unlock the files by demanding a "ransom" (Bridges, 2008). These ransoms are most often demanded in the form of bitcoins, a type of cryptocurrency . When using bitcoins , transactions are irreversible, there is also a low fee of approximately $0.043 USD

per transaction , and the owner of a particular bitcoin account can (Angel and McCabe, 2015). Due to bitcoin's ability to make transactions easy while protecting the anonymity of those involved

, it has become the preference currency for criminal activity including ransomware hackers (Schneider, 2014; Swartz, 2017). According to a November 2015 report by the Cyber Threat Alliance, a single ransomware variant - CryptoWall 3 - was responsible for 406,887 attempted infections and $325 million in damages since it was discovered in January 2015 (

Kumar, 2015).

Based upon these financial estimates, it is believed that new variants of this version of ransomware and other ransomware approaches are certainly being developed and released

(McCarthy, 2016).

In fact, one estimate reports the number of new ransomware variants being developed as 100,000 a day (Pollock, 2016)!In the past, ransomware of attacks had primarily been used to target individuals; however, criminals have the ability to not only encrypt the files on an individual victim's local computer, but they can also encrypt networked files to which that user had

access. This makes organizations a more lucrative target for cybercriminals (Bridges, 2008).

In fact, according to the U.S. Department of Health and Human Service Office for Civil Rights' Breach Portal, which displays breaches of health data that affect 500 or more people, over 325,000 healthcare data breaches were reported (Arndt, 2017) Ransomware is typically spread through fake emails that have been designed by the hacker to appear legitimate (Mustaca, 2014).

These emails may contain a link to an infected website or include an attachment such as a Word document that contains macros. Once a link is clicked or a document is opened, it downloads and infects the machine quickly: estimates vary from seconds (Correa, 2017; NFF, 2017) to 20 minutes (Cybereason, 2016).

During this time, the malware searches the hard drive, network files, external drives, and cloud drives for all files that can be encrypted. After encryption, a "key" is required to unlock the files

; this key is saved by the hacker, and this key in not released until the victim pays a requested amount or "ransom" (Mustaca, 2014).

Prior to 2016, healthcare organizations were not thought to be a primary target for ransomware

(McCarthy, 016). However, hospitals have become an easy target for hackers, for two reasons: (1)

the necessity for computer-stored information associated with patient care e.g., electronic edical records) and (2) the security holes in information technology (IT) systems. In fact, a report from

Ponemon Institute, in 2016 stated that 89% of healthcare organizations suffered at least one data breach involving the loss of patient data over a 2-year period, and 45% had more than 5 such breaches. In addition, the frequency of successful hacking of patient medical files increased from

55% in 2015 to 64% in 2016. When hit with ransomware, some hospitals have been desperate to pay the ransom due to their need to provide critical care to patients with the most up-to-date inform

ation such as drug interaction, care directives, and medical history (Zetter, 2016a). Ransomware

has made it easy for hackers to attack hospitals due to their sudden adaptation of IT without a

concomitant increase in the number and sophistication of IT support staff. This adaptation occurred after the government allocated funds for Meaningful Use, which was used to encourage the use of EHRs. With the Meaningful Use incentive, EHR utilization has increased from 9.4% in 2008 to 96.9% in 2014 (ONC, 2015).

With such a substantial increase in IT utilization in a short time frame, many healthcare facilities

have been unable to adopt adequate network and other information technology resources to combat potential attacks (Verizon, 2016).

Without adequate resources, many hospitals simply do not have the staff to provide simple barriers to hackers such as prompt installation of patches. According to a 2016 report by Verizon, 85% of successful exploits take advantage of vulnerabilities such as outdated patches/

https://works.bepress.com/alberto_coustasse/107/

Задание 3. Суммируйте содержание текста

New Start-Up Company Makes Parking a Whole Lot Smarter!

Whether it's parking at a major event, or just getting into campus, one of the biggest headaches of our daily commute, and sometimes the hardest part is what comes in the end – finding a park-ing spot. SmartRF Solutions, a new startup company founded by Dr. Arijit Sengupta and his business part-ner, provides custom solutions for AVI enabled parking

systems, starting from basic access control systems to complex end-to-end systems for large parking chains.

With the AVI (Automatic Vehicle Identification) technology used in the SmartPark RF product from SmartRF Solutions, the hassles of getting into a parking lot may

get easier for many. For example, faculty and staff at Wright State University

today use AVI in their restricted parking lots courtesy of a research project that is being commercialized into a parking solution that could solve many of the problems with our daily commute.

Such is the case for Katie Halberg, Senior Writer and Editor at Wright State University, who was so thrilled at not having to roll down the window to swipe her card that she wrote a beautiful poem based on Poe's The Raven, excerpts from which are reproduced below with the author's permission:

"From my window, I could see a driver struggle, reaching out his car door

(For the rare and long-armed Raider can reach this and more...)

To swipe their card and open the door....

By that Heaven that bends above up—by that RFID we've come to adore—

Rejoiced this employee as the gate swung upward and upward more,

Without a Wright1 Card, only a parking tag and nothing more....

And my car window shall be lowered—nevermore!"

SmartPark RF can equip an existing parking lot or garage with AVI capabilities. AVI allows vehicles to be automatically identified (leading to allowing/denying access to the structure) without any manual assistance from the operator of the vehicle. This makes parking more efficient, reduces vehicle queue lengths, and increases safety and convenience, because operators do not have to roll down the window or remove their card or wallet to gain access. It also provides easy ADA conformance with seamless access to physically handicapped clients. SmartPark RF can lead to several additional services such as parking space counting, violation detection, and guest parking management. An initial survey of users of martParkRF suggests that over 90% of users would be happy to pay a small $5 surcharge for this service – something that parking management can use to easily derive a return on investment in the technology.

http://corescholar.libraries.wright.edu/cgi/viewcontent.cgi?article=1020&context=infosys_scm

Задание 4. Изложите содержание текста на английском языке используя активную лексику.

60% компаний по ошибке рассылали секретные документы

Евгений Царев

Около 43% организаций считают, что им не хватает ясной политики обеспечения безопасности внутренних документов.

Сначала это была печально известная утечка файлов Агентства Национальной Безопасности с участием Эдварда Сноудена, теперь портал WikiLeaks опубликовал якобы украденные документы ЦРУ: безопасность документов снова в эпицентре событий.

Недавнее исследование, проведенное компанией Business Performance Innovation (BPI) среди более 200 владельцев бизнеса, исполнительных директоров и работников умственного труда, показало, что, хотя большинство из них и обеспокоены возможной утечкой критически важных документов в результате кибератаки, главное беспокойство вызывает случайная отправка конфиденциальной информацией кем-либо из сотрудников.

Согласно исследованию, 61% респондентов беспокоятся о том, что сотрудник отправит конфиденциальную информацию ошибочному адресату, а 41% обеспокоен утечкой важных документов. И самое главное, шесть из десяти опрошенных говорят, что им самим или кому-то из сотрудников уже случалось по ошибке отправлять документы.

Около 43% опрошенных также сообщают, что их компания не имеет ясной политики обеспечения безопасности документов. Это приобретает большое значение, поскольку документы все чаще содержат конфиденциальную информацию. Почти 75% респондентов говорят, что они сами или их сотрудники еженедельно создают документы, содержащие конфиденциальную информацию, и более 33% делают это ежедневно.

«Очевидно, что безопасность документов представляет собой большую и пока не решенную задачу», — говорит Дэйв Мюррей, сотрудник компании BPI Network. «Компании должны лучше обучать своих сотрудников и применять такие утилиты, как связанные документы или «умные PDF-файлы», которые позволяют пользователям шифровать и восстанавливать документы».

Фрэнк Диксон (Frank Dickson), директор по исследованиям компании IDC, отмечает, что даже если нарушение безопасности не исходит из вредоносного источника, это не означает, что оно приносит меньше вреда.

«Случайная утечка все еще является утечкой и может оказаться достаточной серьезной», — говорит Диксон. «Особенно, когда речь идет о способности сотрудников совершать ошибки».

Другие, не менее серьезные причины для беспокойства: передача внешними партнерами конфиденциальных документов без разрешения (34%); документы, разглашенные сотрудниками целенаправленно (33%); уволенные сотрудники, на личных устройствах которых сохранились конфиденциальные документы (26%); недостаточно защищенные документы, выпущенные в обращение (22%).

Что касается последствий похищения или утечки документов, то ответы варьировались от ущерба репутации (53%) до судебных процессов (41%), потери времени и производительности (40%). Еще 39% указали на конкурентные риски, а 34% обеспокоены тем, что подобный инцидент может стоить им работы. И лишь 21% опрошенных обеспокоены потерей дохода.

http://www.securitylab.ru/blog/personal/tsarev/341436.php

Задание 5. Дайте определения основным понятиям: the system development life cycle.

Задание 6. Прокомментируйте следующее высказывание:

Applying the risk management process to system development enables organizations to balance requirements for the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the SDLC. Risk management processes identify critical assets and operations, as well as systemic vulnerabilities across the organization. Risks are often shared throughout the organization and are not specific to certain system architectures.

Контрольная работа
3 курс 6 семестр
Темы 21-22. Информационные системы на предприятии. Уровни управления данными и требования к ним.

Задание 1. Кратко сформулируйте основную идею текста

Cybersecurity professionals are a vital component in combating cyber threats. Cybersecurity professionals are required to have a high level of combined KSAs (i.e. competency) to create and implement

technologies , as well as manage human resources in order to : identify cyber threats and vulnerabilities, protect information and resources, detect the occurrences of cyber security events, respond to incidents, a s well as recover from cybersecurity events (Paulsen et al., 2012; NIST, 2014).

However, most IS users are not cybersecurity professionals, the majority of IS users are lacking awareness as well as training in information technology (IT) and cybersecurity .

Lack of cybersecurity competency of IS users is a critical vulnerability to organizational networks, which is of utmost importance since vulnerabilities are contributing to substantial financial losses for governments and organizations all over the world. To mitigate the cybersecurity KSA shortfalls of IS users, many companies and governments have instituted initiatives such as SETA programs or cyber awareness programs (D'Arcy, Hovav, & Galletta, 2009; DISA, 2015).

http://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1055&context=ccerp

Задание 2. Составьте план текста

Meaning of Business Information System.

Business information systems are sets of inter-related procedures using IT infrastructure in a business enterprise to generate and disseminate desired information.

Such systems are designed to support decision making by the people associated with the enterprise in the process of attainment of its objectives.

The business information system gets data and other resources of IT infrastructure as input from the environment and process them to satisfy the information needs of different entities associated with the business enterprise.

There are systems of control over the use of IT resources and the feedback system offers useful clues for increasing the benefits of information systems to business. The business information systems are sub-systems of business system and by themselves serve the function of feedback and control in business system.

The business information systems are subject to the dynamics of business environment and need to be flexible enough to absorb the inevitable changes in the information needs of business. They have to be efficient to satisfy the demanding and 'hard task masters,' the business managers. Thus, there is need to balance the conflicting objectives in the process of designing business information systems.

Business information systems need to be proactive. They should anticipate changes in information needs of users and accordingly adapt themselves to suit their needs. This has become important because of the fact that the managers get involved in the routine activities to the extent that the decision making becomes a matter of imitating what competitors are doing or planning to do, rather than making an informed choice.

3. The purpose of business information system is to cater to the information needs for decision making in business.

4. The business information systems have to be designed keeping in view the availability of financial and human resources to the business enterprise.

5. The cost effectiveness is a matter of prime concern in the development and maintenance of business information systems. Economic justification for investment in IT infrastructure for business information systems is a pre condition for its existence and sustenance.

Information systems can be described by four of their key components which are:

1. Decisions
2. Transactions and processing
3. Information and its flow
4. Individuals or functions involved.

It is difficult to observe the decision process through we can see and review the results of a decision. Transactions are usually more visible, though many current systems use computer programs, which are not easy to understand, to process transactions. In principle, an observer can see information and its flows. Individuals can be observed too, but it is not always easy to figure out the information processing functions they perform.

http://www.yourarticlelibrary.com/management/information-system/business-information-system-meaning-features-and-components/70319

Задание 3. Суммируйте содержание текста

With the increasing use of web browsers and the rise of The Internet of Things (IoT), developing secure software has become essential in protecting users on the web. Web browsers help users interact with a plethora of web based services. Some of these services include databases and management systems that handle sensitive information, which the integrity of the data and systems can be vulnerable to cyber attacks. A business can no longer risk product delivery turnaround time in exchange for a less secure software product as they risk exposing themselves to corporate espionage, data loss and lawsuits. Developing secure software needs to be considered a requirement and needs to be placed on the same priority level as other system software requirements. Experts claim that the security of browser-based applications is considered less important than speed, functionality and overall experience during developments (Sargent, 2012). Vulnerabilities in HTML 5 make it an emerging threat while SQL injection and XSS remain among the top attacks (OWASP, 2013). Fortunately, researchers have developed a deep understanding of web/browser application threats, and have designed counter measures to mitigate threats, which naturally can become excellent resources to develop valuable education materials. In a study done on ten computer security students it was found that most of them did not do any of the weekly reading assignments and those that did only read about ten minuets(Schreuders & Butterfield, 2016). Therefore, it is imperative to change traditional teaching methods and find ways to engage students in game-like self-paced educational environments that will prepare the future workforce with expertise and skills on web/browser security.

http://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1054&context=ccerp

Задание 4. Изложите содержание текста на английском языке используя активную лексику.

Технологии обеспечения информационной безопасности в современных информационных системах и сетях

Применение защищенных виртуальных сетей.

Internet и другие публичные сети обеспечивают возможность существенно снизить стоимость построения распределенной автоматизированной системы, однако передаваемая по этим сетям информация без принятия дополнительных мер оказывается незащищенной. В связи с этим использование телекоммуникационной среды публичных сетей как части ЗАС требует формирования на их основе защищенных каналов. Это осуществляется с использованием шифрования и контроля целостности передаваемой информации. «Канал» связи между каждой парой удаленных объектов ЗАС, использующих шифрование циркулирующей между ними информации, оказывается закрытым по отношению к внешней среде (если используются стойкие алгоритмы). Таким образом, на основе открытой телекоммуникационной среды оказывается сформированной защищенная сеть, причем никаких затрат на построение физических каналов связи не было произведено. Такие виртуальные сети получили название «Виртуальные частные сети» - VPN (Virtual Private Networks). В настоящее время они приобрели чрезвычайную привлекательность в качестве инструмента организации электронного бизнеса, электронного документооборота, оперативного средства совершения финансовых операций.

VPN - это объединение локальных сетей и отдельных компьютеров, подключенных к сети общего пользования и использующих последнюю как телекоммуникационную среду для передачи шифрованных сообщений, что

обеспечивает конфиденциальность и целостность передаваемой информации между объектами соединенными через открытую сеть общего пользования.

Наложенная корпоративная сеть на сеть общего пользования становится виртуальной защищенной сетью благодаря использованию следующих трех основных элементов обеспечения информационной безопасности:

Шифрование (обеспечение секретности).

Аутентификация (проверка подлинности, включая контроль целостности, и придание юридической силы передаваемым сообщениям).

Контроль доступа.

Только реализация этих трех механизмов позволяет защитить пользовательские компьютеры, серверы предприятия и данные, передаваемые по незащищенным каналам связи, о нежелательных внешних вторжений, утечки информации и несанкционированных действий.

Технология VPN предусматривает комплексную защиту передаваемых данных: при создании VPN-канала проверяется аутентичность двух сторон, создающих канал, а затем каждый пакет переносит цифровую подпись, сформированную отправителем и удостоверяющую аутентичность и целостность пакета; для обеспечения конфиденциальности пакеты шифруются, причем для сокрытия адресной информации, раскрывающей внутреннюю структуру сети, пакеты могут быть зашифрованы вместе с заголовком и инкапсулироваться во внешний пакет, несущий только адрес внешнего интерфейса VPN-шлюза.

В настоящее время для организации защищенных VPN-каналов используется комплекс стандартов Internet, известный под названием IP-Sec (IP Security). Стандарты IP-Sec характеризуются универсальностью и гибкостью. В этих стандартах оговорены обязательные для аутентификации и шифрования протоколы и алгоритмы, что обеспечивает базовую совместимость IPSec-продуктов, и в то же время разработчик IPSec-продукта может дополнять данный список другими протоколами и алгоритмами, что делает возможным постоянное развитие системы безопасности. Для аутентификации сторон и генерации сеансовых ключей в стандартах IP-Sec предусмотрена возможность

использования цифровых сертификатов и структуры открытых ключей PKI (Public Key Infrastructure), что делает решение IP-Sec

масштабируемым и согласованным с другими средствами защиты, например со средствами контроля доступа.

Средства VPN могут эффективно поддерживать защищенные каналы трех основных типов (варианты применения):

С удаленными сотрудниками (защищенный удаленный доступ).

С сетями филиалов предприятий (защита intranet).

С сетями предприятий-партнеров (защита extranet).

Для защита удаленного доступа важно наличие клиентских частей VPN для основных клиентских операционных систем. От шлюза VPN в этом варианте требуется хорошая масштабируемость для поддержания сотен и даже тысяч защищенных соединений. При защите сети extranet главным требованием является соответствие реализации VPN-продуктов стандартам IP-Sec. Следует заметить, что поддержка IP-Sec сегодня является обязательным условием для перспективных VPN- продуктов. http://www.iz-news.ru/lect/472/

Задание 5. Дайте определения основным понятиям из области информациннной безопасности: the information system lifecycle.

Задание 6. Прокомментируйте следующее высказывание: As companies become more reliant on modern technology, they also have to face more vulnerabilities that must be handled efficiently.

Контрольная работа
3 курс 6 семестр
Темы 23-25. Планирование информационных систем. Организационная защита информации. Комплексная система защиты информации на предприятии.

Задание 1. Кратко сформулируйте основную идею текста

The exponential growth of the Internet, the convergence of Internet and wireless multimedia applications and services pose new security challenges. Security is a complex system and must be considered at a ll points and for each user. Organizations need a systematic approach for information security management that addresses security consistently at every level. They need systems that support optimal allocation of limited security resources on the basis of predicted risk rather than perceive d vulnerabilities. However, the security infrastructure of most organizations came about through necessity rather than planning, a reactive-based approach such as detection of vulnerabilities and applying software updates is opposed to a proactive approach. On the other hand, cyber security plans call for more specific requirements for computer and network security as

well as emphasis on the availability of commercial automated auditing and reporting mechanisms and promotion of products for security assessments and threat management.

Besides technical security controls (firewalls, passwords, intrusion detection, disaster recovery plans, etc.), security of an organization includes other issues that are typically process and people issues such as policies, training, habits, awareness, procedures, and a variety of other less technical

and non-technical issues. Security education and awareness has been lagging behind the rapid and widespread use of the new digital infrastructure.

All these factors make security a process which is based on interdisciplinary techniques. The existing challenges of information security management combined with the lack of scientific understanding of organizations' behaviors call for better computational systems that support effectiveness of using specific information technologies and new approaches based on intelligent techniques and security informatics as means for coordination and information sharing. Intelligent systems emerged as new software systems to support complex applications.

In this paper, we propose the architecture for an Intelligent System for Information Security

Management (ISISM) which supports the security processes and infrastructure within an organization. Among these components, intelligent systems include intelligent agents that exhibit a high level of autonomy and function successfully in situations with a high level of uncertainty. The system supports knowledge acquisition that is likely to assist the human user, particularly at deeper levels of comprehension and problem solving for the information security assurance domain.

http://proceedings.informingscience.org/InSITE2007/IISITv4p029-043Hent387.pdf

Задание 2. Составьте план текста

When one examines a complete enterprise, the number of threats and vulnerabilities rapidly soars. Implementing a series of point solutions for each of these different cases is viewed as unsustainable. When faced with a whole bunch of blood thirsty mosquitoes, one has a couple of choices. Kill them one at a time, or in small groups, or move to a different control mechanism (like taking refuge in a car) and exclude them from your reality. Yet, systems theory shows the flaws associated with believing in one size fits all solutions. Endpoint based solutions with highly targeted regulator functions can act very efficiently and with high degrees of specificity against threats. The challenge is to balance numbers of solutions versus unrealistic expectations of single one size fits all solutions.

Systems level theory and thinking opens these opportunities up to designers, moving from the realm of designing numerous similar point solutions to more comprehensive control mechanisms that address the problem from a different angle. People are managed through policies, yet an examination of how this regulator operates demonstrates that it will not be effective against several types of users. Users that are ignorant of the policy will break it not out of malice, but ignorance. Training and awareness will fix some of

these, but how effective is this line of defense? Policies may not be enforceable against all parties. Once an employee has decided that they are leaving, whether for another job or not, many of the penalties associated with policies have little strength. Senior management members, those with the greatest span of control over information are also least likely to be directly affected. Either because of position or parachute clause, senior executives are not driven by fear from policies. Contract workers, workers with a

grievance, temporary workers – each has its own of these are accurately modeled into the control mechanism of the regulator. The rule from requisite variety, that the regulator must have as many control states as the system can have in its operation is applicable here. How many different states can executives, disgruntled employees, temporary workers, etc. exist inside a policy driven system? What are the requisite levels and numbers of controls against the diverse group? Designing the system for the typical employee will work against them, but is this really the threat one desires protection from?

Systems level thinking, backed by an understanding of systems theory is a valuable new way of examining issues and applying the correct balance of solutions. The use of these concepts as tools to assist designers to understand the ramifications of design choices will result in better more secure designs. The concept of regulator scope and environmental boundary relationships are aspects of the security problem that are many times overlooked or brushed aside with sweeping thoughts of it can be fixed with a few more rules. Understanding the true nature of the limitations of a regulator function based on system size brings a notion of reality and theory based foundation into play.

The use of systems level thinking reveals many interesting things about designing security. Examining threats against a system as a collection of individual items in isolation does not provide an appropriate level of information to properly craft a strong defense. In addition to just enumerating the threat and its mechanism, an understanding of the system level that it is invoking will enable the security designer to employ multiple layers of appropriate defenses Proceedings of the 41st Hawaii International Conference on that have an ability to impact the threat. Threat modeling is a relatively new technique designed to help security professionals understand and communicate critical issues concerning threats, vulnerabilities and mitigating actions. But this is an analysis of only one side of the equation.

Balancing out the threat side is a systems level analysis of the defensive side, where the range of control of regulators and security control boundaries are placed.

Systems employed in a modern business environment today are rarely created from the ground up. Most are enhancements and modifications to previous systems, expansions and changes to even major components as the business shifts and morphs the IT infrastructure to meet the dynamic demands of the business place. This ever changing landscape demands a good understanding of all aspects of the security equation, both from the threat side and the defensive side. With this understanding, it becomes possible to keep security in the picture as a system is upgraded to meet future challenges, both from business needs and security needs.

Developing and maintaining a comprehensive set of systems theory based maps detailing security mechanisms and the effects of boundaries, regulators and the actual elements being regulated will enable security architects to examine entire systems. With this type of information, it can be seen where defense in depth is actually occurring and where it isn’t.

These diagrams can also assist in the understanding of complex security appliances that are comprised of multiple independent devices on the inside. Both dependent and independent security mechanisms can be mapped and understood. Not only does this increase the simplicity of a previously complex system, it also can expose security system weaknesses that may be obscured by complex designs.

The addition of systems theory understanding adds another tool to the toolbox for designers, developers, architects and security professionals. Systems theory provides a basis for understanding the ramifications of how things work and what the relationships are between a system, its environment and how much can be controlled. This being said, systems theory is not a be all, end all, solution to the myriad of problems facing the security community.

https://www.computer.org/csdl/proceedings/hicss/2008/3075/00/30750265.pdf

Задание 3. Суммируйте содержание текста

As modern business organizations increase their reliance on information systems to meet the challenges of the competitive marketplace, the importance of security becomes an important issue. Designing security solutions in today's diverse computing and growing threat environment is a challenging and complex task.

Security can act as a control mechanism in a system. Security mechanisms are designed to allow desired events and block undesired ones. When computer systems were simple and single purpose in nature, the design of control mechanisms to provide for security was a relatively simple and well understood task.

As the use of computer systems in business expanded in the past several decades, so have the number of application, including e-mail, office automation programs, accounting programs, and databases. The Internet expanded the scope of the problem further, with the addition of e-commerce, instant messaging, web sites, web services and more. During the period of expansion in function came the era of system consolidation and system integration. Major vendors began offering suites of solutions to various business problems. This combination of application integration, server consolidation and enhanced business services was designed to increase business efficiency, productivity and business responsiveness. The simplifications offered by these changes did not extend to security functionality.

During the same period, the threat to information systems has changed dramatically, from an age of simple network attacks designed to demonstrate hacker prowess, to today's integrated and sophisticated botnet attacks designed to specifically defraud companies and users. Increasing levels of attacks have lead to more frequent security breaches, and the losses associated with them has resulted in a heightened level of importance to company executives. Recent surveys have indicated that the majority of organizations consider information security as highly important to achieving their overall business objectives. Information security vendors and researchers have responded to the changes through the development of a wide range of technology based solutions.

Technology based solutions and research have been based on point solutions, with

differing answers for access control, encryption, and protective devices such as firewalls and intrusion detection systems. The myriad of point solutions have lead security professionals to navigate a complex minefield of options and capabilities. Guides to deployment strategy exist through a series of principles, such as defense in depth. The result has been a patchwork and piecemeal deployment of a diverse set of technological solutions in an attempt to secure the enterprise.

The result, when measured against the growing list of security incidents is proving to be less than desired. An examination of the problem through the lens of systems theory provides some interesting models of understanding of this complex problem.

Systems theory has been applied to many areas of study, and systems engineering approaches have guided many firms in their security offerings.

The use of systems theory in this way will provide information to designers, developers, and security professionals in their attempt to understand the limitations and basis for limitations with respect to this critical functional aspect of their systems. This is the application of what has been described as 'hard' systems theory as opposed to 'soft' methodologies by Checkland and others.

https://www.computer.org/csdl/proceedings/hicss/2008/3075/00/30750265.pdf

Задание 4. Изложите содержание текста на английском языке используя активную лексику.

Организация защиты информации на предприятиях (в организациях, учреждениях)

Предприятия (фирмы, организации, учреждения) - наиболее многочисленные структуры, в которых создается наибольший объем (количество) информации, содержащей государственную и конфиденциальную тайну. В них проводится конкретная и разнообразная работа по защите информации.

Независимо от формы собственности организация для проведения работ с информацией, содержащей государственную тайну, должна получить лицензию, т. е. выполнить предварительно в полном объеме требования по защите информации, предусмотренные соответствующими документами. После получения лицензии организация становится элементом государственной системы защиты информации, содержащей государственную тайну.

Для защиты информации, содержащей государственную тайну, на предприятии (в учреждении, организации) создаются в зависимости от объема работ по защите информации структурные подразделения или штатные специалисты, которые могут входить в состав одного из подразделений или службы безопасности. Их основными функции являются следующие:

* планирование работ по защите информации на предприятии (в учреждении, организации), разработка предложений по совершенствованию его системы защиты информации;

* определение демаскирующих признаков предприятия (учреждения, организации) и выпускаемой продукции;

· участие в подготовке предприятия (учреждения, организации) к аттестованию на право проведения работ с использованием сведений, отнесенных к государственной тайне;

* организация разработки нормативно-методических документов, разработка проектов распорядительных документов по вопросам организации защиты информации на предприятии;

· участие в согласовании ТЗ (ТТЗ) на проведение работ, содержащих государственную тайну, в разработке требований по защите информации при проведении исследований, разработке (модернизации), производстве и эксплуатации образцов продукции, при проектировании, строительстве и эксплуатации объектов (учреждения, организации);

* проведение периодического контроля эффективности мер защиты информации на предприятии (в учреждении, организации), участие в расследовании нарушений в области защиты информации и разработка предложений по устранению недостатков и предупреждению нарушений;

* организация проведения занятий с руководящим составом и специалистами предприятия (учреждения, организации) по вопросам защиты информации.

Для защиты информации, составляющей коммерческую тайну, ее владелец создает собственную систему защиты информации.

Законодательно структура такой системы не закреплена. Она определяется многими факторами: видом деятельности, уровнем конфиденциальности информации и ее объемом, штатной численностью ее сотрудников, финансовым состоянием фирмы и др. Однако для любой фирмы однотипны объективные функции сил и средств обеспечения защиты информации. Их может выполнять как полноценная структура, включающее большое количество людей и технических средств, так и несколько человек для малой фирмы. В принципе, так же как в государственных структурах, каждый сотрудник фирмы должен в объеме должностных обязанностей обеспечивать защиту информации. Об этом он информируется при приеме на работу. Эти требования указываются, как правило, в договоре между работодателем и работником.

Система безопасности фирмы образует следующие основные элементы (должностные лица и органы):

· руководитель фирмы, курирующий вопросы безопасности информации;

совет по безопасности фирмы; служба безопасности фирмы;

подразделения фирмы, участвующие в обеспечении безопасности фирмы.

Руководство безопасностью возлагается, как правило, на руководителя фирмы и его заместителя по общим вопросам (первого заместителя), которому непосредственно подчиняется служба безопасности.

Совет по безопасности фирмы представляет собой коллегиальный орган при руководителе фирмы, состав которого назначается им из числа квалифицированных и. ответственных по вопросам информационной безопасности должностных лиц. Совет безопасности разрабатывает для руководителя предложения по основным вопросам обеспечения безопасности информации, в том числе: направлениям деятельности по обеспечению безопасности фирмы и ее подразделений, совершенствования системы безопасности, взаимодействия с органами власти, заказчиками, партнерами, конкурентами и потребителями продукции и др.

Структурные подразделения занимаются вопросами защиты информации, которую они создают или используют в своей деятельности. Содержание и количество информации меняются во времени, в зависимости от решаемых задач и этапов деятельности. Однако основные и побочные результаты деятельности содержат защищаемую информацию еще длительное время, равное времени ее старения.

Служба безопасности является основным структурным подразделением по обеспечению безопасности, в том числе информационной, на фирме. Основными ее задачами в части информационной безопасности являются:

· мониторинг угроз информации;

* организация работы по защите информации на фирме;

· управление доступом сотрудником, автотранспорта и посетителей на территорию и в помещения фирмы;

* обеспечение безопасности информации при проведении всех видов деятельности внутри и вне фирмы, в том числе при чрезвычайных ситуациях;

* охрана территории, зданий, помещений и других мест и конструкций с защищаемой информацией.

Кроме этих задач служба безопасности обеспечивает охрану материальных ценностей фирмы и безопасность руководителей, ведущих специалистов и сотрудников.

http://pandia.ru/text/77/158/16343.php

Задание 5. Дайте определения основным понятиям из области информациннной безопасности: information systems planning.

Задание 6. Прокомментируйте следующее высказывание: Information systems security begins at the top and concerns everyone.

Контрольная работа
4 курс 7 семестр
Темы 26-27. Угроза информации. Система управления рисками.

1. Задание 1. Кратко сформулируйте основную идею текста

COMMERCIAL SECURITY SYSTEMS FOR THE DIGITAL AGE

John Moran Director at Minerva Security

The best commercial security systems will be a step ahead of the people who are trying to breach the security systems in question. This isn't an easy task. The people who are trying to break into commercial security systems usually try to devise ways of doing so as something of a full-time job. The people who are trying to maintain the security around their businesses will usually only be doing so as a part-time job. Fortunately, it is possible to stay one step ahead of time.

Even in the digital age, it is still important to make sure that a given location is secured. People are going to need security cameras for their businesses in addition to all of the security measures that they're going to need for all of their digital information. In fact, in some cases, security cameras and alarm systems can still help businesses catch digital thieves, assuming that they need to make contact with the corporate building at any given time. However, companies are usually going to have less and less of a need for physical assets with time, and most of the security measures that they need today are going to be digital in nature.

So many people believe that having everything backed up on the cloud is the answer. Indeed, having data backed up on the cloud provides some important preventative measures when it comes to natural disasters and equipment failures. However, releasing so much of that information on the cloud is also going to create a situation in which people can access information that would have been completely out-of-reach otherwise. Grabbing information from the cloud is becoming increasingly common in a world in which digital information is simultaneously becoming more vigorously protected but also more broadly available.

One of the best defenses against hackers has always been encryption. Many of the best hackers can still get around some of the firewalls that people set up, but it's going to take them much longer, which is going to increase the likelihood that they're going to be caught in the act or that they're going to have to start over, giving people the time they need in order to intervene at the right moment. Encryption codes and encryption software keeps on getting better and better, so companies are going to make sure all of those codes and that software is as up-to-date as possible, or people are going to find themselves falling behind in the race against the hackers.

Sometimes, the best solution is active monitoring. On the cloud network side, there should be anti-hackers working to make sure that nothing happens. If hackers are working almost non-stop to find a way into a system, there needs to be a corresponding group of people that will be working just as hard in order to make sure that these people don't gain access to the necessary systems. High-quality software can still make a difference in these situations, but the software itself can be subject to the activities of the hackers. It's more important to make sure that there is an additional line of defense outside of software.

Commercial security systems can also involve other pragmatic measures. Companies that are able to divide their important data among many different servers are going to run into a frustrating situation if it turns out that they have to rely on the backups. All of the information is going to be divided among several different servers, setting themselves up for a tough recovery process. However, doing so is still a good idea from the perspective of cybersecurity. Even if hackers do manage to get past all of their active monitoring and encryption software, they're still going to run into a situation in which they don't really gain access to much data. If the data is divided among several different servers, individual servers will be far less vulnerable to intrusions, and a break-in is going to be less damaging.

Commercial security systems for the digital age are certainly becoming more complicated. Hackers and the people designing protective software are in a veritable competition. This competition is ongoing. Companies don't really get rewards: they just get the opportunity to maintain. However, this is a necessity in this day and age.

Задание 2. Составьте план текста

SOCIAL MEDIA AND BYOD ARE BIGGEST INTERNAL SECURITY THREATS

Steve Evans Freelance journalist, copywriter and editorial consultant

Access to social media and BYOD are the biggest internal security threats businesses face, while organized cybercrime is the greatest external threat, according to a new report from fraud specialists Callcredit Information Group.

The group's *Fraud and Risk 2016 Report* found that fraud prevention managers and directors rated employee access to social media websites and services (43%) and BYOD to work (35%) as the biggest obstacles IT faces when it comes to preventing data breaches. Lack of knowledge about security threats (28%) and access to personal email accounts (25%) are also considered problematic.

As well as being worried about those internal threats, fraud managers also fear external risks. Organized cybercrime is listed as the current biggest threat, with 75% of respondents fearing it. Respondents to the survey were also worried about identity fraud (51%), money laundering (50%) and social engineering, such as phishing (46%).

However, many appear to see organized crime as a short-term issue; only 26% think organized crime will still be as big a threat in two or three years. Instead, denial of service is expected to be the primary external threat in the future, ahead of "malicious, external loss or compromise of data" (50%), and "accidental, internal loss or compromise of data by an employee" (50%), and ransomware (48%).

Fraud managers seem particularly worried about internal threats. More respondents (46%) considered the threat of malicious, internal loss of data or fraud by an employee a greater threat than the same threats from external parties (42%).

Despite these worries, many fraud managers feel their organization is ahead of those cyber-criminals who specialize in fraud. Just 13% feel they are behind the fraudsters, while 75% feel on top of things.

The report also brought up interesting reactions to Brexit. While most respondents (57%) feel it will have little impact on the risk of fraud, 28% feel it will increase it. That's primarily driven by a fear that leaving the EU will reduce information sharing between the UK and European anti-fraud authorities.

"As fraud in our society grows, and as geographically mobile individuals increasingly need to establish their digital identity, so the pressure on fraud and risk professionals to protect their organizations and consumers mounts," said John Cannon, director, fraud & ID, Callcredit Information Group.

"Whilst fraud professionals might be confident in their abilities to prevent and deal with a potential breach, our research suggests that employees need much more education on the risks. Explaining the threats, giving them suggestions on how to protect themselves and informing them about ways to spot a breach could be instrumental in protecting a company from cybercrime. Organizations are only as strong as their weakest link, and the entire workforce needs to understand what the cyber vulnerabilities are in order to prevent them," he added.

Задание 3. Суммируйте содержание текста

IOT WOES: SIMPLISAFE HOME SECURITY

Tara Seals US/North America News Reporter, Infosecurity Magazine

The internet of things continues to widen the attack surface: A vulnerability in SimpliSafe's home security system gives an attacker full access to the alarm at a time of his/her choice in the future.

According to IOActive, due to the design of the home security system, all keypads and base stations will need to be replaced in order to secure the system.

"We are seeing a growing trend where companies launching 'internet of things'–enabled products to market either forget or choose to exclude security as part of the product's design and development," said IOActive researcher Andrew Zonenberg, in an analysis. "The end result is that these products can be easily compromised by hackers with malicious intentions in mind. This is particularly alarming when the products are intended and marketed for security purposes."

The SimpliSafe system consists of two core components, a keypad and a base station. These can be combined with a wide array of sensors, ranging from smoke detectors to magnet switches to motion detectors, all connected wirelessly.

An attacker armed with a commodity microcontroller board, SimpliSafe keypad and SimpliSafe base station (an investment of about $250) can build a device that records the code that's used to unlock communications between the elements. It can then spoof the legitimate device to arm or unarm the system.

"The attacker can hide the device anywhere within about a hundred feet of the target's keypad until the alarm is disarmed once and the code recorded," Zonenberg explained. "Then the attacker retrieves the device. The code can then be played back at any time to disable the alarm and enable an undetected burglary, or worse."

Normally, the vendor would fix the vulnerability in a new firmware version by adding cryptography to the protocol used. But that's not an option for the affected SimpliSafe products because the microcontrollers in currently shipped hardware are one-time programmable, the researcher explained.

"This means that field upgrades of existing systems are not possible; all existing keypads and base stations will need to be replaced," he said. Considering that SimpliSafe says that there are 1 million+ systems already installed, the cost to mitigate this for the vendor is not going to be cheap.

Zonenberg that he tried several times to contact the vendor with no response, and that IOActive reported the issue to CERT.

SimpliSafe is not the only home security system in the spotlight of late. Earlier in the year, a vulnerability was discovered in Comcast XFINITY's Home Security System that could open the door—literally—to intruders.

Задание 4. Изложите содержание текста на английском языке используя активную лексику.

ТЕРМИНОЛОГИЯ УПРАВЛЕНИЯ РИСКАМИ НА ОБЩЕДОСТУПНОМ ПРИМЕРЕ

Vlad Styran

Управление рисками многие считают очень сложным и неприятным занятием. Это неправда. Управление рисками -- это естественный и непрерывный процесс, происходящий в мозгу каждого человеческого существа. Процесс настолько привычный, что большую часть времени мы его даже не замечаем.

Чтобы определиться с терминами в этой области, давайте рассмотрим пример: пешеход пересекает проезжую часть. Пешеход (пусть это будет старушка) в нашем примере составляет актив, а проезжая часть наполнена вечно куда-то мчащимися угрозами -- автомобилями. Давайте усложним задачу и предположим, что на нашей улице по три полосы в каждую сторону.

К этому моменту мы уже определили актив и угрозы. Осталось выяснить, как нам обеспечить безопасность бизнес-процесса, то есть перевести бабушку через улицу. Риск столкновения бабушки и ~~мчащегося по крайней левой со скоростью 80+ км/ч~~ автомобиля является для нас неприемлемым, поэтому мы применяем контроли (они же контрмеры) этого риска.

Контроль №1: пешеходный переход, регулируемый светофором. В этом случае у старушки периодически будет появляться "окно" в 1-2 минуты, в течение которых вероятность столкновения будет достаточно невелика, чтобы отважиться на пересечение улицы. Но с техническими контролямивсе не так просто: иногда они ломаются. В этом случае у нас есть...

Контроль №2: "зебра", то есть характерная разметка, а также дорожные знаки пешеходного перехода. Если светофор не работает, для всех участников движения переход считается нерегулируемым, то есть, на нем преимущество имеют пешеходы. Как показывает практика, эффективность такого контроля по-меньше, поэтому он называется компенсационным.

Контроль №3дополняет картину в административнойплоскости: это правила дорожного движения, с которыми (предположительно) ознакомлены все участники движения и за нарушение которых агенту угрозыгрозит серьезное наказание.

Итак, в такой системе рисков и контролей для нашего актива станет возможной наиболее безопасная стратегия течения бизнес-процесса: переходить улицу в положенном месте и на разрешающий сигнал светофора. В надежде на то, что все водители соблюдают ПДД.

P.S. В идеальном мире первым делом была бы рассмотрена возможность устранения угрозы, то есть постройки над- или подземного перехода. Не всегда это решение является приемлемым, в основном по причине своей дороговизны. Поэтому от момента возникновения необходимости в пешеходном переходе до момента его постройки проходит какое-то время, за

которое фонарные столбы неподалеку от этого участка улицы плотно обрастают искусственными венками.

Задание 5. Дайте определения основным понятиям из области информациннной безопасности: information security threats.

Задание 6. Прокомментируйте следующее высказывание:

Companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer, operate and account for computer systems that contain protected information.

Kevin Mitnick

Контрольная работа
4 курс 7 семестр
Темы 28-29. Требования к обеспечению безопасности. Защита коммерческой информации

Задание 1. Кратко сформулируйте основную идею текста

NSA DIRECTOR TO HEAD UP CIS CONTROLS

Tara Seals US/North America News Reporter, Infosecurity Magazine

Curt Dukes, former director of information assurance at the National Security Agency (NSA), has been named the Center for Internet Security (CIS) executive vice president.

Dukes will be responsible for managing the Security Best Practices Automation Group, which includes the CIS Security Benchmarks, the CIS Controls and the tools to automate the evaluation of the standards.

"Curt Dukes' three decades of senior executive leadership and his unparalleled track record of pioneering and managing complex cybersecurity products and services make him an ideal leader for the Security Best Practices Automation Group," said John Gilligan, CIS board chair and interim CEO. "His addition will accelerate our efforts to provide our nation with effective solutions to address rapidly growing cybersecurity challenges."

Dukes also will focus on the expansion of the content of CIS standards and increased adoption of CIS security best practices and standards. He will also lead the development and delivery of effective tools for scoring the implementation of CIS Benchmark and Controls standards and for automating the implementation of security best practices.

The CIS Controls are a concise, prioritized set of practices that outline what every organization should do as their first steps in cybersecurity. They have been proven to mitigate 85% of the most common vulnerabilities.

One of the benefits of the CIS Controls is they are developed by experts based on their first-hand experience in the security field and are derived from actual threat data from a variety of public and private sources. In addition to being prioritized and relevant, the CIS Controls are updated regularly to stay in step with cybersecurity's ever-changing threat environment.

"The cybersecurity industry is about innovation, and CIS is already a well-positioned leader in transforming security technology for today's increasingly connected businesses," said Dukes. "I am excited to join CIS as executive vice president and look forward to helping the Security Best Practices Automation Group continue its impressive track record of innovation and growth," he added.

Dukes has served as the director of information assurance at the National Security Agency in Fort Meade, Md., since 2013. His responsibilities included the security of systems that handle classified information or are otherwise critical to the US military or intelligence activities.

From 2007 to 2013, Dukes was director of the NSA/Central Security Service (CSS) Commercial Solutions Center, where he was responsible for leading the agency's portal to the commercial world. His responsibilities included leveraging industrial relationships, while partnering with international and national

intelligence communities, and the Department of Defense, to address the strategic needs of the NSA/CSS and the National Security community.

From 2004 to 2007, Dukes was NSA's chief at the Systems and Networks Analysis Center, where he led a technical workforce providing technology risk assessments, cyber-defense operations and advanced vulnerability research.

Dukes earned an MS in Computer Science from Johns Hopkins University after completing a BS in Computer Science at the University of Florida.

Задание 2. Составьте план текста

EMPLOYEES ARE SHARING CONFIDENTIAL INFO AT ALARMING RATES

Tara Seals US/North America News Reporter, Infosecurity Magazine

Nearly three in four employees (72%) are willing to share sensitive, confidential or regulated company information, and more than one in three employees say it's common to take confidential corporate data with them when leaving a company.

Those alarming stats are from the Dell End-User Security Survey, which found that not only are many employees likely to share confidential information, but that they are doing so without proper data security protocols in place or in mind.

Results show that today's workforce is caught between two imperatives: be productive and efficient on the job and maintain the security of company data. To address data security issues, companies must focus on educating employees and enforcing policies and procedures that secure data wherever they go, without hindering productivity. So far, they're falling down on the job: A full 76% of employees feel their company prioritizes security at the expense of employee productivity.

Survey results indicate that among the professionals who work with confidential information on a regular basis, there is a lack of understanding in the workplace regarding how confidential data should be shared and data security policies.

"This lack of clarity and confusion is not without merit; there are many circumstances under which it makes sense to share confidential information in order to push business initiatives forward," the report noted. This opens the door to a wide range of reasons for sharing which include: Being directed to do so by management (43%); sharing with a person authorized to receive it (37%); determining that the risk to their company is very low and the potential benefit of sharing information is high (23%); feeling it will help them do their job more effectively (22%); feeling it will help the recipient do their job more effectively (13%).

The survey found that when employees handle confidential data, they often do so insecurely by accessing, sharing and storing the data in unsafe ways; Almost half (45%) of employees admit to engaging in unsafe behaviors throughout the work day. These include connecting to public Wi-Fi to access confidential information (46%), using personal email accounts for work (49%) or losing a company-issued device (17%).

About a quarter (24%) of respondents indicated they do these things to get their job done, and 18% say they did not know they were doing something unsafe. Only 3% of respondents said they had malicious intentions when conducting unsafe behaviors.

"When security becomes a case-by-case judgement call being made by the individual employee, there is no consistency or efficacy," said Brett Hansen, vice president of Endpoint Data Security and Management at Dell. "These findings suggest employees need to be better educated about data security best practices, and companies must put procedures in place that focus first and foremost on securing data while maintaining productivity."

Four in five employees in financial services (81%) would share confidential information, and employees in education (75%), healthcare (68%) and federal government (68%) are also open to disclosing confidential or regulated data at alarmingly high rates. Employees take on unnecessary risk when storing and sharing their work, with 56% using public cloud services such as Dropbox, Google Drive, iCloud and others to share or back-up their work; and 45% of employees will use email to share confidential files with third-party vendors or consultants.

Ironically, nearly two in three employees (65%) feel it is their responsibility to protect confidential information, including educating themselves on possible risks and behaving in a way that protects their company, and 36% of employees feel very confident in their knowledge of how to protect sensitive company information.

Nearly two in three (63%) employees are required to complete cybersecurity training on protecting sensitive data. However, of those who received cybersecurity training, 18% still conducted unsafe behavior

without realizing what they were doing was wrong, whereas 24% conducted unsafe behavior anyway in order to complete a task.

"While every company has different security needs, this survey shows how important it is that all companies make an effort to better understand daily tasks and scenarios in which employees may share data in an unsafe way," said Hansen. "Creating simple, clear policies that address these common scenarios in addition to deploying endpoint and data security solutions is vital in order to achieve that balance between protecting your data and empowering employees to be productive."

Задание 3. Суммируйте содержание текста

TO MINIMIZE THE DAMAGE CAUSED BY BREACHES, DATA MUST BE EFFECTIVELY LOCKED DOWN

Rreze Halili Training Course Developer, PECB International

The huge number of components, devices and users, and the enormous volume of data that is created, transmitted and saved every day, mean that organizations must manage complex systems. Every day these systems are subject to different types of attack against the sensitive information of clients, employees, and confidential business data.

Despite the evolution of technology, management protection systems within companies, awareness plans, and massive investments against hackers and cyber-attacks, organizations continue to be threatened.

In fact this condition is spreading. The Ponemon Institute found that in 2014 the average cost to a company from a data breach was up 15% from the previous year. Attackers have become even more dangerous, using the help of social engineering, sophisticated automated tools and a wide range of other methods. Malicious and criminal attacks were the most costly types of cybercrime to a business, the study found.

Years ago, companies used to keep these incidents and breaches secret to save reputation and the loss of customers, suppliers, and partners. But lately companies and information security professionals have started to accept that data breaches are often impossible to prevent.

Now an organization's information security posture should consider risk resilience and incident response plans in order to manage and mitigate the damaging impacts of data breaches. There are already some methods that intend to help organizations with such issues.

First, organizations need to know about their data sensitivity (the kind of data they have and how important it is). They need to apply policies and regular audits on how to access data, remove the parts they do not need, protect the sensitive elements and ensure what is left is well organized and easily searchable.

Sensitive, high-value documents such as customer records, intellectual property and contracts need special treatment. The growing volume of data and different media, devices and systems used as storage devices makes the locking-down process complicated.

One way to lock data down is to use encryption techniques to secure the confidentiality, availability, integrity and nonrepudiation of data just for intended users. Encryption techniques are used to secure safe transfer from one storage place to another, then to secure data within storage systems within organizations and also to secure data in storage systems like the cloud.

Another method is to use tools that will enable privileged management and access rights for the document and files. This can be done by using passwords which will allow only the right users to have access to specific data.

Moreover, in order to keep data secure, attention should be paid to the download process of different applications. Applications should be downloaded only from the secure sources which are known as official application stores. Downloaded applications from insecure sources can infect devices with malware and viruses.

In conclusion, data breaches will happen, so to successfully manage data, effective solutions should be used, locking the data down in a way which keeps it secure. Even if a company is subject to a data breach, saved data will still be safe and the attacker will not have be able to have access and gain information. This will minimize the damage that can be done.

Задание 4. Изложите содержание текста на английском языке используя активную лексику.

ПОЛЬЗОВАТЕЛИ ЗАПАДНОЙ ЕВРОПЫ И СЕВЕРНОЙ АМЕРИКИ ПОД УГРОЗОЙ КРАЖИ ФИНАНСОВОЙ ИНФОРМАЦИИ

Эксперты «Лаборатории Касперского» подготовили отчет о самых распространенных киберпреступлениях в Западной Европе и Северной Америке за первое полугодие 2012 года. Специалисты отмечают, что большинство интернет-пользователей чаще всего устанавливают на свои устройства антивирусное ПО, однако это не останавливает кибермошенников, которые разрабатывают все более сложные вредоносные программы.

В отчете «Лаборатории Касперского» указывается, что зачастую европейские и североамериканские пользователи становятся жертвами троянских программ, целью которых является хищение финансовых средств. Эксперты разделили трояны, использующиеся в западных странах, на четыре группы:

- программы, которые доставляют и скрывают вредоносное ПО;
- похищающие данные трояны;
- многофункциональные трояны;
- вымогающие деньги трояны.

В первой половине 2012 года 70% атак с использованием троянов на пользователей из США, Канады и Западной Европы проводилось при помощи бэкдора Sinowal (Mebroot). 41% нападений приходился на универсального трояна SpyEye и почти четверть на банковскую вредоносную программу Zeus.

Еще одной распространенной угрозой, которой подвергаются пользователи из Северной Америки и Западной Европы, является кража личных данных. Причиной хищения персональной информации являются уязвимости и ошибки в настройке серверов и баз данных, а также бреши в конфигурации веб-приложений. После кражи личных данных мошенники продают их на форумах или используют для получения неправомерного доступа к различным финансовым сервисам.

Злоумышленники нередко используют трояны-вымогатели, которые после заражения блокируют доступ к компьютеру, изменяя системные настройки или открывая свое окно поверх всех остальных. Зачастую такие угрозы используются в странах СНГ, так как европейские граждане сразу обращаются в полицию по факту вымогательства. Однако в настоящее время злоумышленники придумали другой прием для обмана европейцев: они блокируют компьютер и якобы от имени полиции требуют оплатить штраф за посещение сайтов, содержащих детскую порнографию или сцены насилия над детьми.

: http://www.securitylab.ru/news/429970.php

Задание 5. Дайте определения основным понятиям из области информациннной безопасности: *commercial classified information.*

Задание 6. Прокомментируйте следующее высказывание:

> *Our information network is much better protected than our railroad network, and someone who cracks a system is able to cause far less human damage than someone who derails a train. Why, then, has 'computer crime' caused so much hysteria? Perhaps because the public is so willing - eager, even - to be scared by bogeymen.*
>
> Charles Platt

Контрольная работа
4 курс 8 семестр
Темы 30-31. Экономическая составляющая информационной безопасности. Информационная безопасность и интеграционные процессы

Задание 1. Кратко сформулируйте основную идею текста

BACKLASH: HALF OF CONSUMERS TAKE BUSINESS ELSEWHERE POST-BREACH

Tara Seals US/North America News Reporter, Infosecurity Magazine

With major data breaches making what seem like daily headlines, attention is turning to the aftermath of those hacks and the toll they take on the executive suite and the bottom line alike. New research shows that companies are paying a steep price when customers' information is compromised: more than half of all respondents, 51%, will take their business elsewhere after a breach.

A snap poll conducted by HyTrust shows that household names, such as retailers Home Depot, Target, Goodwill and Neiman Marcus, as well as individual banks, healthcare organizations, insurance companies and ISPs, are all vulnerable to consumer backlash. In particular, customers are likely to churn in the event of a compromise of personal information, including address, social security number and credit card details.

More than a third of respondents, 34.2%, believe that the worst piece of information to be compromised is the social security number (SSN).

The number of people that will talk with their wallets and take their business elsewhere jumps to 60.2% among consumers in the 35 to 44 age range—a key consumer demographic.

Customers feel victimized as well: a full 45.6% said that the companies involved in such a breach should be considered criminally negligent the moment a breach occurs, with the majority also believing that all officers of a company should be held responsible. Famously, this is what happened at Target, which saw a few of its C-suite depart in the wake of last year's catastrophe.

When asked who in particular should be held ultimately accountable for failures in information security, 19.7% of respondents don't make a distinction between executives with varying responsibilities, pointing the finger at "all officers" of a company. However, men and women aged 25 to 34 identify CSOs as most responsible, while those in the 45 to 54 age bracket go easiest on them.

"There probably isn't a single straw that broke the camel's back—it's just the sheer volume of stories about data breaches, many at companies that have developed a customer-friendly brand," said Eric Chiu, president at HyTrust, in a statement. "What this poll shows is that companies are finally, and inevitably, being held to account for their security vulnerabilities. Consumers have options, and when there are endless stories about the loss of confidential information, they're going to other vendors. Every security breach clearly has a direct impact on operations, but there's now clear evidence that extensive brand damage happens as well, and the executives involved will have to pay the price."

Further, it would appear that there is little wiggle room: most consumers (45.6%) blame the companies involved the moment a data breach occurs, while only 12% withhold condemnation until 'it happens more than once.' Additionally, this finger-pointing increases with age, with 34% of 25-34 year olds laying immediate blame versus 51% of those 65 and up.

Interestingly, the more consumers make, the more forgiving they tend to be; the top answer for those making $150,000 or more shifted to 'when it happens more than once.'

Higher earners are also more concerned about their SSNs: 36.5% of those making $50,000 to $74,000 per year cite this potential theft as most serious, while that falls to 22.8% among those making $24,000 or less.

Задание 2. Составьте план текста

KASPERSKY TACKLES CRITICAL INFRASTRUCTURE WITH EMBEDDABLE SYSTEM

Tara Seals US/North America News Reporter, Infosecurity Magazine

IT systems are increasingly the lifeblood of vertical businesses, thus demanding enhanced cybersecurity to avoid economic (or worse) meltdowns in the event of a compromise. To that end, Kaspersky Lab has announced the Kaspersky Security System platform, a dedicated solution for information systems like ERP and electronic document management systems, smart grids, the internet of things (IoT) and critical infrastructure. It's available as an embeddable OEM component to manufacturers and vendors of comprehensive IT solutions for these applications.

Kaspersky Security System's key features include its ability to apply access control rules according to given security policy, classify the informational resources and configure the interaction of the components.

"An analysis of the evolution of trends in cybercrime suggests that any information system without a trusted infosecurity module poses a threat to the security and integrity of business processes, and may potentially lead to serious consequences," said Andrey Doukhvalov, head of future technologies and chief strategy architect at Kaspersky Lab, in a statement. "This is what drives our team to continuously improve our IT security knowledge and solutions. With this new product, we help our partners make their IT systems more trusted and reliable without affecting their safety. Kaspersky Security System is a platform with a unique component makeup and feature set. It ensures the required level of cybersecurity for any IT system with demanding security requirements."

Meanwhile, SYSGO and Kaspersky Lab have integrated the new platform into the real-time operating system PikeOS. Combined with PikeOS, Kaspersky Security System ensures that performed communications comply with security policies. It can be used in industrial systems to protect devices at the supervisory and control (SCADA) level, in connected IoT devices to assure their proper behavior, and in automotive systems

to separate the safety-critical subsystems from infotainment components connected to the Internet, among others.

"By teaming up with Kaspersky Lab we bring IT security to embedded systems," said Knut Degen, CEO of SYSGO, in a statement. "With the integration of Kaspersky Security System into PikeOS we can deliver a high-performance solution that will help our joint customers to secure their devices in the Internet of Things."

The OEM component is designed to integrate into information systems, and is suitable for use by software and hardware vendors, as well as system integrators. The vendor or integrator can apply basic, default security policies or manually fine-tune their security configurations to meet the requirements presented by specific systems or business tasks.

Задание 3. Суммируйте содержание текста

CONGRESSIONAL REPORT: US POWER GRID UNDER CONTINUOUS CYBER-ASSAULT

A survey of 112 of the top 150 national utilities by US Reps. Edward Markey (D-Mass.) and Henry Waxman (D-Calif.) painted a picture of continuous assault, using techniques that range from phishing to malware infection to unfriendly probes.

Markey and Waxman noted that "Cyberattacks can create instant effects at very low cost and are very difficult to positively attribute back to the attacker. It has been reported that actors based in China, Russia, and Iran have conducted cyber probes of US grid systems, and that cyberattacks have been conducted against critical infrastructure in other countries."

More than one public power provider reported being under a "constant state of 'attack' from malware and entities seeking to gain access to internal systems." A Northeastern power provider said that it was "under constant cyber-attack from cyber criminals including malware and the general threat from the Internet." And, a Midwestern power provider said that it was "subject to ongoing malicious cyber and physical activity. For example, we see probes on our network to look for vulnerabilities in our systems and applications on a daily basis. Much of this activity is automated and dynamic in nature – able to adapt to what is discovered during its probing process."

While the hackers seem to have been thus far unsuccessful – none of the utilities reported specific damage to any of their computer systems – the parameters for sharing information are lacking, the report found.

"There did not appear to be a uniform process for reporting attempted cyberattacks to the authorities; most respondents indicated that they follow standard requirements for reporting attacks to state and federal authorities, did not describe the circumstances under which these requirements would be triggered, but largely indicated that the incidents they experienced did not rise to reportable levels," Markey and Waxman wrote.

The survey did find a high compliance rate with mandatory standards issued by the North American Electric Reliability Corporation (NERC), but providers are less likely to have implemented NERC's voluntary recommendations.

For example, NERC has established both mandatory standards and voluntary measures to protect against the computer worm known as Stuxnet, a sophisticated bug that was used to shut down centrifuges at Iranian nuclear facilities. Of those that responded, 91% of investor-owned utilities, 83% of municipally or cooperatively owned utilities, and 80% of federal entities that own major pieces of the bulk power system reported compliance with the Stuxnet mandatory standards. By contrast, of those that responded to a separate question regarding compliance with voluntary Stuxnet measures, only 21% of IOUs, 44% of municipally or cooperatively owned utilities, and 62.5% of federal entities reported compliance.

Hackers may not spend very much to attack the grid, but the potential consequences are staggering. The US bulk-power system serves more than 300 million people, is made up of more than 200,000 miles of transmission lines, more than 1 million megawatts of generating capacity, and is valued at over $1 trillion. The vast majority of grid assets are owned and operated by private companies and other non-federal institutions. The components of the grid are thus highly interdependent, and a line outage or system failure in one area can lead to cascading outages in other areas, with catastrophic effects.

"For example, on August 14, 2003, four sagging high-voltage power lines in northern Ohio brushed into trees and shut off," the report noted. "Compounded by a computer system error, this shut-down caused a cascade of failures that eventually left 50 million people without power for two days across the United States

and Canada. This event, the largest blackout in North American history, cost an estimated $6 billion and contributed to at least 11 deaths."

Задание 4. Изложите содержание текста на английском языке используя активную лексику.

НЕ ВСЕ БАНКИ ГОТОВЫ ПЕРЕЙТИ НА НОВЫЕ СТАНДАРТЫ КИБЕРБЕЗОПАСНОСТИ

К концу текущего года банки обязаны провести самооценку своего соответствия новым нормам.

В прошлом году международная система передачи банковской информации и осуществления платежей SWIFT использовалась хакерами для похищения крупных сумм из целого ряда банков по всему миру. Для предотвращения будущих кибератак было принято решение усилить безопасность SWIFT, и уже менее чем через месяц начнется проверка финансовых организаций на соответствие новым нормам.

Как сообщает «РБК», не все банки готовы принять новые стандарты. По мнению глав IT-отделов крупных финорганизаций, изменения могут повлечь за собой большие траты, проблемы с технической стороной вопроса и угрозу репутации.

Руководитель SWIFT по России, СНГ и Монголии Матвей Геринг на днях напомнил банкам о переходе на новые стандарты безопасности. По словам специалиста, 1 апреля будут опубликованы 27 контрольных пунктов – 16 обязательных и 11 рекомендуемых. К концу текущего года финансовые организации обязаны самостоятельно оценить свое соответствие новым нормам. Данные о не соответствующих стандартам банках будут переданы регуляторам. Это касается не только российских участников рынка, но и всех организациях, использующих SWIFT.

Новые нормы предполагают дополнительные требования к антивирусным решениям, обеспечению и проверке целостности ПО и баз данных, квалификации и организации работы специалистов, а также к местам хранения устройств. Новые требования касаются процесса выявления аномальной активности в SWIFT и введения двухфакторной аутентификации.

По словам одного из источников «РБК», для соответствия новым требованиям придется перенастраивать всю IT-систему. Если процесс перенастройки затянется, работать с системой будет невозможно, поскольку с 1 сентября следующего года прекратится поддержка необновленных SWIFT.

Как сообщают банкиры, с наименьшими рисками в связи с переходом на новые требования столкнутся организации, являющиеся непосредственными участниками международных платежных систем (Visa, MasterCard и пр). Остальные же (особенно небольшие и региональные банки) столкнутся с гораздо большими рисками, поскольку им придется реализовывать требования SWIFT с нуля, уверен глава IT-отдела финорганизации из топ-100. Установка, обновление и обеспечение ПО и БД может обойтись среднему банку в довольно приличную сумму – 10-15 млн руб.

Могут также возникнуть трудности с выполнением требования по повышению осведомленности сотрудников. Как показывает практика, тренинги и обучение являются неэффективными, и персонал по-прежнему использует ненадежные пароли, хранящиеся на бумажках на рабочем месте.

Алексей Коняев, старший консультант SAS Россия/СНГ по решениям для обеспечения безопасности и противодействия мошенничеству

То, что SWIFT всерьез взялось за разработку собственных стандартов безопасности, безусловно, является правильным решением, однако, как представляется, немного запоздалым. К слову сказать, международные карточные платежные системы такие, как VISA или Mastercard, уже давно разработали и применяют в своей деятельности собственные стандарты безопасности, которые, кстати говоря, во многом пересекаются с новыми правилами SWIFT. В этой связи, банкам, которые имеют прямые договорные отношения с МПС и которые, как следствие, обязаны выполнять их требования по безопасности, не должны испытать серьезных сложностей в части соблюдения стандартов SWIFT.

Однако таких банков не так уж и много, и более того – это, как правило, крупные банки, для которых это и так не должно было стать большой проблемой. Серьезные трудности могут возникнуть у остальных – ведь процесс адаптации к данным стандартам потребует от организаций существенных усилий и материальных затрат.

При этом шансов не выполнять или игнорировать новые правила по всей видимости нет. Мировая практика тех же международных платежных систем показывает, что это может обернуться крупными штрафами для таких организаций. С другой стороны менеджмент SWIFT в России настроен серьезно и обещает не только сообщать в ЦБ о банках, невыполняющих требования по безопасности, но и принимать смелые решения вплоть до отключения от системы при грубых нарушениях.

Подробнее: https://www.securitylab.ru/news/485377.php

Задание 5. Дайте определения основным понятиям из области информациннной безопасности: *information in business terms*.

Задание 6. Прокомментируйте следующее высказывание:

We need to make sure that leaks of classified information, of national security secrets, needs to be rigorously pursued and prosecuted to the fullest extent of the law.

John O. Brennan

Контрольная работа
4 курс 8 семестр
Темы 32-33. Прикладная экономика. Информационная экономика.

Задание 1. Кратко сформулируйте основную идею текста

UK ISP SAYS DIGITAL ECONOMY ACT IS PAST ITS SELL-BY DATE

Tara Seals US/North America News Reporter, Infosecurity Magazine

The Digital Economy Act was the brainchild of Lord Mandelson during the last Labour government. It was rushed into law via the controversial 'wash-up' process at the end of that parliament – meaning it received very little parliamentary debate. It has remained a controversial Act ever since.

The Act includes a controversial '3 strikes' provision, but has required guidance from Ofcombefore it can be brought into force. Ofcom's draft code for consultation was published last month, just before the European Parliament rejected ACTA and its own graduated response provisions. "If a customer receives three letters or more within a 12-month period", says Ofcom, "anonymous information may be provided on request to copyright owners showing them which infringement reports are linked to that customer's account. The copyright owner may then seek a court order requiring the ISP to reveal the identity of the customer."

DEA contains further provisions that could "require ISPs to take steps (such as internet bandwidth reduction, blocking internet access or temporarily suspending accounts) against relevant subscribers in certain circumstances", says Ofcom. Its announcement starts, "Internet users will be encouraged to download music and films through legal channels under measures outlined today by Ofcom," prompting Jim Killock, Chief Executive of the Open Rights Group to suggest "Ofcom are being asked to put lipstick on a pig with this code." Darren Farnden, head of marketing at Entanet, agrees with Killock: "Pursuing people through the courts based on shaky IP address information and then threatening them with warning letters and disconnection is not the way to tackle this issue."

Ofcom's own timetable indicates that DEA measures will not start until at least 2014. It is this that prompts Entanet to suggest it can no longer be effective. "With so much notice," says Farnden, "surely the most prolific infringers will have discovered even more ways to circumvent the DEA by the time it's enforced." In particular he points to the use of VPNs and proxies. "The most commonly talked about circumvention techniques are the use of proxies or VPNs. Research by the Cybernorms research group at the Lund University in Sweden revealed a 40% rise in the use of VPN systems by the 15 to 25 year age group since 2009 in Sweden, surely proof that such circumvention is already being implemented."

Farnden points to a contradictory healthy growth in legal online music sales. He quotes the 2012 IFPI Digital Music Report, which states: "Many major markets are seeing healthy increases in single track download sales, including the US, up 10 per cent (Nielsen SoundScan); the UK, up 8 per cent (Official Charts Company/BPI) in 2011; and France up 23 per cent (GfK). Consumer demand for iTunes, the market leader, is growing healthily." This prompts Farnden to conclude that "Entertainment companies need to reassess their business models to take advantage of the opportunities the Internet brings, not fight them."

Задание 2. Составьте план текста

CHECK POINT, CISCO JOIN CYBER THREAT ALLIANCE

Tara Seals US/North America News Reporter, Infosecurity Magazine

The Cyber Threat Alliance (CTA) has added Check Point Software Technologies and Cisco as alliance founding members.

It also has appointed Michael Daniel as the organization's first president, and announced its formal incorporation as a not-for-profit entity.

The existing founding members are Fortinet, Intel Security, Palo Alto Networks and Symantec. Together, the six founding Members have contributed to the group's first project: The development of a new, automated threat intelligence sharing platform to exchange actionable threat data, further driving the CTA's founding mission of fomenting a coordinated effort against cyber-adversaries.

The CTA's corporate purpose as a not-for-profit is to share threat information across member organizations and protect customers; to advance the cybersecurity of critical IT infrastructures; and to increase the security, availability, integrity and efficiency of information systems.

In addition to expanding its founding members, the CTA's affiliate members, include IntSights, Rapid7 and RSA, who join existing members Eleven Paths and ReversingLabs.

Since its inception in 2014, the CTA has regularly exchanged information on botnets, mobile threats and indicators of compromise (IoCs) related to advanced persistent threats (APTs), and advanced malware samples. Notable milestones of the CTA's cooperative efforts cracked the code on CryptoWall version 3, one of the most lucrative ransomware families in the world, totaling more than US $325 million ransomed. The CTA's research and findings pushed cybercriminals to develop CryptoWall version 4, which the CTA also uncovered and resulted in a much less successful attack.

The CTA platform automates information-sharing in near real-time to solve the problems of isolated and manual approaches to threat intelligence. The platform better organizes and structures threat information into Adversary Playbooks, pulling everything related to a specific attack campaign together in one place to increase the contextual value, quality and usability of the data. This approach turns abstract threat intelligence into actionable real-world protections, enabling members to speed up information analysis and deployment of the intelligence into their respective products.

To foster continued collaboration and incentivize meaningful threat data, the new CTA platform requires members to automate their intelligence sharing contributions, meet a minimum contribution every day, and rewards contextualized, unique intelligence. Members will eventually be rewarded with greater levels of access based on the value and volume of the information they have contributed.

"The future of cyber security is here. The CTA collaboration will enable us to accelerate the pace of innovation as we work to protect the cloud, mobile and provide the best means for advanced threat prevention," said Gil Shwed, founder and CEO, Check Point.

Задание 3. Суммируйте содержание текста

AN ARGUMENT IN FAVOR OF LICENSING INFORMATION SECURITY PROFESSIONALS

Rreze Halili Training Course Developer, PECB International

In today's complex and interconnected information age, with much mention of cloud, big data, mobility, social business, and cybersecurity, individuals and organizations require assurance that the systems that have become part of their everyday lives are trustworthy, reliable and secure.

Currently, it is impossible to turn to a licensed individual (or group) to obtain this assurance, in much the same way that one can enlist the services of licensed professionals such as lawyers, accountants or doctors. The main reasons one would turn to these professionals is that a license proves the individual:

- Is a member of and governed by a recognized professional association
- Is licensed to practice (i.e., has the required education, knowledge, skills and experience)
- Adheres to widely accepted standards and practices
- Is held accountable for their actions through being governed by codes of professional conduct and disciplinary processes

Being licensed and part of a professional organization also demonstrates that the individual complies with mandated continuing education requirements and is part of a professional community – possibly global –

that engages in knowledge sharing and is actively involved in keeping up to date with current developments in their chosen field.

Licensing will likely become mandatory for information security as we move into the 'internet of everything', including interconnected household devices, autonomous cars and e-medicine. Advances like these are on the horizon and will significantly increase the reliance we place on technology. People's lives will quite literally be at stake; in fact, this is already the case.

Given the impact on our everyday lives and potential implications for public safety, the need for licensing people who design and implement security will be as significant a need as licensing for engineers who design our buildings and infrastructure, or doctors who look after our health. The potential for harm will be too great to trust security to just anyone who has managed to land a job but who may not have the necessary skills, education or experience.

With continued focus on information security and cybersecurity in particular, we are very likely to see increased pressure to procure information assurance and security services only from licensed individuals. It is important to note that professional certifications from leading global organizations that have strong credentialing programs already meet much of the licensing requirements. Indeed, many government agencies worldwide already have a form of licensing by mandating that certain services can only be performed by certain credential holders. A licensing program could, therefore, easily leverage the efforts of existing certification organizations that have years of experience in developing training and certifications, and are already accredited by recognized standards bodies such as ANSI and ISO, to establish the standard for information security professionals.

One particular challenge is likely to be the national interests of individual countries. Although technology and information systems don't really recognize international borders, cybersecurity and national security interests – a key driver for licensing – are likely to be country-specific. However, other licensed professions have found ways of coping with international mobility and global workforces, and no doubt so will the licensed information security professionals of the future.

As an information security professional working in a large global financial services organization with complex information security challenges, and as an individual with genuine concerns about the privacy and security of my own personal data, I would like to make a strong case for information security professionals to be licensed much like other professions. Overall, licensing will engender safer and more secure environments for doing business and lead to increased trust in, and value from, information systems.

If you want a health check of your information systems, you should be able to turn to a licensed information security professional.

Задание 4. Изложите содержание текста на английском языке используя активную лексику.

ЭКСПЕРТЫ: ЭЛЕКТРОННЫЕ УСТРОЙСТВА ВЕДУТ МИР К ЭНЕРГЕТИЧЕСКОЙ КАТАСТРОФЕ

Чтобы избежать коллапса правительства разных стран должны предпринять незамедлительные меры по ужесточению стандартов потребления электрической энергии электронными устройствами.

Международное агентство по энергетике International Energy Agency (IEA) призывает правительства разных стран должны предпринять незамедлительные меры по ужесточению стандартов потребления электрической энергии электронными устройствами.

Эксперты считают, что если такие меры не будут предприняты, к 2030 г. электронные устройства во всем мире будут потреблять втрое больше электрической энергии, чем сейчас. В связи с этим проблемы безопасности энергетических систем и проблемы с выбросом парниковых газов выйдут на новый уровень. «Текущая работа по улучшению электрических характеристик различных электронных приборов является недостаточной. Технологии развиваются быстрее и сводят на нет все продвижения в данной области», - говорит Нобуо Танака (Nobuo Tanaka), исполнительный директор IEA.

В настоящий момент на электронные устройства приходится 15% всей энергии, потребляемой одной квартирой или домом. Однако это значение быстро растет, в основном из-за роста спроса на такие устройства в Африке и других странах с развивающейся экономикой. Так, например, на сегодняшний день в мире работает почти 2 млрд телевизоров. Более половины жителей Земли пользуются мобильными телефонами, которые требуют постоянной подзарядки. Согласно прогнозу IEA, в течение следующих 7 месяцев число постоянных пользователей персональных компьютеров превысить отметку в 1 млрд человек.

Если тенденция сохранится без ужесточения стандартов, к 2030 г. гаджеты будут потреблять 1,7 петаватт (1700 тераватт) электрической энергии в час, столько же, сколько сейчас потребляют все домохозяйства в США и Японии вместе взятые, комментирует Танака. Сумма всех счетов за электроэнергию достигнет $200 млрд. Для того чтобы обеспечить электроэнергией все новые и старые гаджеты к 2030 г. потребуется нарастить мощность электростанций на 280 ГВт.

Однако, используя современные технологии, потребление электрической энергии пользовательских устройств можно сократить более чем в два раза. «Существенного сокращения электрической мощности устройств можно достичь за счет оптимизации программного обеспечения под то оборудование, для которого оно предназначено», - говорят в IEA.

Так, например, банальная функция периодической проверки почтового ящика на мобильном телефоне ведет к увеличению потребляемой энергии. Компании должны проявлять большее внимание и тратить более значительные суммы для того, чтобы подобные приложения были максимально эффективными с данной точки зрения. Однако здесь не обойтись без помощи государства, так как именно оно может заставить производителей работать в этом направлении.

http://www.securitylab.ru/news/379582.php

Задание 5. Дайте определения основным понятиям из области информационной безопасности: *digital economy*.

Задание 6. Прокомментируйте следующее высказывание:

> *Our information network is much better protected than our railroad network, and someone who cracks a system is able to cause far less human damage than someone who derails a train. Why, then, has 'computer crime' caused so much hysteria? Perhaps because the public is so willing - eager, even - to be scared by bogeymen.*
>
> Charles Platt

2.2 Материалы для проведения промежуточной аттестации:

3 семестр

1. Вид промежуточной аттестации -**зачет с оценкой**
2. Форма проведения - **устный опрос**
3. Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию:

Перечень статей на английском языке для обсуждения с экзаменатором:

1. The decline of music piracy holds lessons for other industries
2. Forget university! It's a PRETTY FACE that helps guarantee a successful career
3. Employment Rates for University Graduates
4. Bellying up to environmentalism
5. Are You Stressed At Work?
6. How to feed the world
7. Mobile marvels
8. Overcoming stress
9. Family life and relationships 'are being damaged by pressures of work'
10. The proof of the pudding
11. Middle-class struggle
12. Moving in with Grandma

Перечень ситуаций для комментирования

1. Imagine that your friend/your colleague/your boss is sure that in the times of severe economic competition stress at work is unavoidable. Try to convince him/her that one can live a stress-free life if they stick to some simple recommendations.
2. Imagine that a friend of yours has been under a lot of stress recently and it is beginning to tell on their health. Advise them on how they should organize their time/activities at work/while studying.
3. Do you agree that nowadays unemployment is not only an economic issue but a social problem as well? How do you think you can persuade your younger friend to make the right choice and choose the career that can help them to avoid being unemployed?
4. Imagine that your former classmate is suffering from stress and anxiety as the exams are due in the next couple of weeks but he/she has fallen behind with the group. What do you think s/he should/should not do to improve the situation?
5. Imagine that as a result of a month's internship you have gained some experience and come to understand that it is not so easy for a beginning specialist to start a career even if you have a university degree. Explain what else you need in order to succeed.
6. Imagine that that your friend has fallen ill with flu but keeps attending classes. Try to persuade him/her to stay at home until they get better. Explain why it may be dangerous for him/her and others.
7. Imagine that as an experienced IT specialist you are invited to a group of University students to give a talk about your work and the job requirements in your company. Try to explain to them that they should not only obtain academic knowledge but also gain the practical skills they need in order to make a career and to succeed in the future.
8. Imagine that your friend is very unhealthy due to eating junk food and smoking cigarettes. He/she also stays up till late at night and does not exercise enough. Persuade him/her to change the way he/she is living as it may lead to health related problems.
9. Imagine that your younger brother/sister/friend is about to leave school but has not made his/her mind about the future. Would you advise them to follow your example and choose a career in IT? Explain why.
10. Imagine that you visit your friend who after having a car accident is undergoing treatment for serious injuries in hospital. Say what could have caused the accident and how the visit affected you.
11. Imagine that you are a newly appointed leading specialist in charge of an IT department. Give your new colleagues instructions about their daily responsibilities. Say what their musts and mustn'ts are.

12. Imagine that your younger brother/sister/friend is suffering from toothache as his/her tooth needs filling. They put off visiting the dentist as they are afraid of pain. Persuade them to visit the dentist as soon as possible

Перечень тем по дисциплине для беседы с экзаменатором

1. What difficulties are usually associated with starting a career? How should a young specialist start looking for a job?
2. Whose role is more important in providing health services – that of the government or of the private sector?
3. What problems does the Russian health sector face nowadays?
4. Speak about the most challenging social problems in present-day Russia.
5. Why did Erik Gorin come to see Professor Fox? What impression did Erik make on Professor Fox? What did Erik learn from Professor Fox about his future work and studies?
6. What did Erik tell Professor Fox about his summer and why? What helped Erik to overcome all his difficulties that summer? What is your impression of Erik Gorin?

7. Who was Mr. Cowlishaw and what kind of practice did he buy? What is your impression of Mr. Cowlishaw?
8. Why did Rannoch choose Mr. Cowlishaw as his dentist? Did Mr. Cowlishaw like the patient's scheme? Did he fall in with the scheme? Why? What is your impression of Rannoch?
9. Who was Mr. Cowlishaw's second visitor? What was she like? What is your impression of Mrs. Clowes?
10. Why was Mr. Cowlishaw glad to have Mrs. Clowes as his first patient? Did his attitude to the situation change later? Describe the operation and how it all ended.
11. Why did Rannoch call Mr. Cowlishaw "one of those amateurs"? What did the words "amateur" and "professional" mean to Rannoch? And to Mr. Cowlishaw?
12. Speak about a good (professional) headhunter's behaviour during his\her first call. What he\she should (or shouldn't) do?Dwell on the potential candidate's behaviour during the call made by the headhunter. Enumerate the recommendations that a candidate should follow during the first interview.

4 семестр

1. Вид промежуточной аттестации – **экзамен**
2. Форма проведения - **устный опрос**
3. Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию:

Перечень статей на английском языке для обсуждения с экзаменатором:

1. 'A crisis of masculinity': men are struggling to cope with life
2. Old CEOs can learn a few new tricks from Lady Gaga
3. Women in science: equality is impossible unless society shifts
4. Squeezing in a conference call between classes
5. Report: Unemployment High Because People Keep Blowing Their Job Interviews
6. Racist behaviour is declining in America
7. How Can You Cope With Stress at Work
8. Business Reputation
9. Beat Your Personal Best: Why You Should Be Your Only Competition
10. Female peacekeepers take the helm, to end gender-based violence
11. Women and Armed Conflict
12. The Importance of Business Reputation

Перечень высказываний для комментирования:

1. Art, freedom and creativity will change society faster than politics.
2. Fairness is what justice really is.
3. Punishment is justice for the unjust.
4. The safety of the people shall be the highest law.
5. It is better to risk saving a guilty man than to condemn an innocent one.
6. The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom.
7. Society exists only as a mental concept; in the real world there are only individuals.
8. War is the continuation of politics by other means.
9. Just because you do not take an interest in politics doesn't mean politics won't take an interest in you.
10. No science is immune to the infection of politics and the corruption of power.
11. At his best, man is the noblest of all animals; separated from law and justice he is the worst.
12. The power of the lawyer is in the uncertainty of the law.

Перечень тем по дисциплине для беседы с экзаменатором:

1. How did it happen that Jackson lost his job? How did his lawyer explain the failure of the case?
2. What was the result of Avis's investigation?
3. Why was Mrs. Packletide so eager to procure a tiger-skin? Was she really interested in hunting?
4. Can you think of another title to the story «Mrs. Packletide's Tiger»? Give reasons for your choice. What traits of human character does the author ridicule in the story about Mrs. Packletide? What is the author's attitude towards his characters?
5. Do you agree that the problems in Enid's family life arose due to some generation gap? Do you think Enid was capable of changing her life?
6. Why do you think Enid was incapable of changing her life? Was there any way out?
7. How would you account for John Harcourt's behaviour in the department store? Do you think he was smitten with remorse?
8. How did Grace behave during the quarrel with John? How do you think the incident affected their relations?
9. Why do you think there was argument between fighters as to whether Spitfire Johnny was dead or alive?
10. Why was the Colonel so carried away by the mystery of Spitfire Johnny? Why did he make up his mind to investigate the case?
11. Are you interested in modern art? Do you often visit galleries and exhibitions?
12. What did Mozart mean when he said, “Composing doesn't become easier with time, but harder, I want more from it, I have to have more”?

5 семестр

1. Вид промежуточной аттестации - *зачет с оценкой*
2. Форма проведения - **устный опрос**
3. Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию:

Перечень статей на английском языке для обсуждения с экзаменатором:

1) Apple Safari Privacy Cookie Features».
2) « Many current publications dealing with cyber security …».
3) The aim of information security…
4) From information security to cyber security
5) Clifton wrote that ‘one man’s information is another man’s data’…
6) A constant flow of information
7) The idea of getting computers to communicate…
8) Theory is one thing, practice quite another
9) It is important that security policy…
10) Information Security Policy (ISP) is …
11) An information security policy is the cornerstone…

Перечень статей на русском языке для обсуждения с экзаменатором:

1) 45% ИТ- ШНИКОВ КРАДУТ ДАННЫЕ КОМПАНИЙ
2) 24 ОКТЯБРЯ НЫНЕШНЕГО ГОДА РОССИЙСКИЕ… .
3) СКРЫТЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
4) Цифровые следы, или почему отсутствует онлайн-конфиденциальность

5) Изменения в кибер-преступлениях в 2017 году
6) Верно ли предприятия оценивают внутренние угрозы?
7) Увольнение за разглашение защищаемой информации
8) Конфиденциальные данные…
9) Что нужно, чтобы стать администратором систем безопасности
10) Большинство сотрудников готовы делиться конфиденциальной информацией
11) Печальный факт дня: большинство людей все еще не знают

Перечень тем по дисциплине для беседы с экзаменатором:

1. Information as the basic element of the security system.
2. Information security.
3. A company's information security.
4. The system of decision-making at a company.
5. Corporate information content management.
6. Information security ethics.
7. The quality management system.
8. A company's information security models.

2 курс 6 семестр

1. Вид промежуточной аттестации - **экзамен**
2. Форма проведения - **устный опрос**
3. Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию:

Перечень статей на английском языке для обсуждения с экзаменатором:

1. Apple safari privacy cookie features».
2. «The aim of information security is…».
3. CYBER-SECURITY: TENSE TOPIC FOR IT PROS TO DISCUSS WITH THEIR BOSSES
4. RED ALERT BANKING MALWARE STEALS CREDENTIALS
5. FINANCIAL ATTRACTIVENESS OF RANSOMWARE ENSURES IT REMAINS GROWING THREAT
6. HACKERS REWRITE JIMMY NUKEBOT MALWARE TO CHANGE ITS GOALS AND TASKS
7. If you could break into your company systems, what would you do?
8. INSIDER THREATS, ACCESS RIGHTS MANAGEMENT AND THE GDPR
9. WHY EU DATA PROTECTION WILL STILL APPLY TO POST-BREXIT UK
10. FIRMS QUESTION PROPOSED EU DATA PROTECTION NOTIFICATION DEADLINE, FINES

Перечень статей на русском языке для обсуждения с экзаменатором:

1. SOFTLINE МОДЕРНИЗИРОВАЛА СИСТЕМУ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЛАСТНОЙ БОЛЬНИЦЫ В ИРКУТСКЕ
2. КИБЕРТЕРРОРИЗМ ОПАСНЕЕ, ЧЕМ БОМБЫ
3. ПОЧЕМУ КОМПАНИИ НЕ ДОЛЖНЫ БОЯТЬСЯ ВВЕДЕНИЯ ОБЩЕГО РЕГЛАМЕНТА ПО ЗАЩИТЕ ДАННЫХ (GDPR)
4. К 2022 ГОДУ В РОССИИ ПОЯВИТСЯ СВОЯ ОС ДЛЯ «ИНТЕРНЕТА ВЕЩЕЙ»
5. GARTNER: EDR-РЕШЕНИЯ НАБИРАЮТ ПОПУЛЯРНОСТЬ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ
6. РОССТАНДАРТ СОЗДАЛ КОМИТЕТ ДЛЯ СТАНДАРТИЗАЦИИ «УМНЫХ» ТЕХНОЛОГИЙ
7. Влияние блокчейн на информационную безопасность
8. ТОЛЬКО АКТИВНЫЙ ПОИСК УГРОЗ ПОЗВОЛИТ ПРОТИВОСТОЯТЬ КИБЕРПРЕСТУПНИКАМ
9. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ИДЕТ РУКА ОБ РУКУ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
10. Компания Forrester Consulting изучила затраты на защиту корпоративной информации

Перечень тем по дисциплине для беседы с экзаменатором:

1. Information as a company’s asset.
2. Information systems.
3. Information systems planning.
4. A company’s information systems.
5. Modern technologies and information security.
6. The information system’s life cycle.
7. Data management levels.
8. Organisational information security.
9. The complex information security system of a company.

4 курс 7 семестр

1. Вид промежуточной аттестации - **экзамен**
2. Форма проведения - **устный опрос**
3. Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию

Перечень статей на английском языке для обсуждения с экзаменатором:

1) Massive wave of ransom DDOs threats sweeps globe
2) Global cost of cybercrime soars 23% in a year
3) The hand that rocks the IoT is the hand that rules the world
4) Smartphone WI-FI searches offer massive new data leakage vector
5) File-sharing, cloud apps leading to more data leakage for companies
6) To manage risk effectively, unconventional controls are
7) ISF updates risk assessment tools
8) Time to get quick on your feet: navigating the network security minefield
9) Malware stats show implemented security isn't effective security
10) 30% of NHS trusts hit by ransomware

Перечень статей на русском языке для обсуждения с экзаменатором:

1) Детские сайты тоже стали заразными

2) Зарядка смартфона как угроза утечки информации
3) Нарушение конфиденциальности информации – самая большая внутренняя ИТ-угроза
4) Малый бизнес: тенденции в защите информации
5) Почему управление рисками не работает?
6) Управление рисками с учетом человеческого фактора
7) Ликбез: классификация угроз
8) Слежка и прослушка телефонов обойдется всего в несколько тысяч долларов
9) Netwire вернулся и крадет платежные данные
10) "Доктор веб": под угрозой находятся персональные данные более 122 тысяч пользователей соцсетей.

Перечень тем по дисциплине для беседы с экзаменатором

1. Information security threats
2. IT risk assessment, risk calculation and evaluation
3. IT risk management
4. IT risk management systems
5. Assessment of the threats and vulnerabilities
6. Types of information damage and
7. Commercial classified information
8. Personal data and methods of their protection
9. Political and industrial espionage
10. Corporate data management
11. Security controls and standards

4 курс 8 семестр

1. Вид промежуточной аттестации - **экзамен**
2. Форма проведения - **устный опрос**
3. Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию:

Перечень статей на английском языке для обсуждения с экзаменатором:

1) NUMBER OF FEDERAL INFORMATION SECURITY WORKERS EXPECTED TO DOUBLE IN FIVE YEARS
2) THE CYBERSECURITY CHALLENGES FACING STATE AND LOCAL GOVERNMENTS
3) Security experts welcome UK government's £1.9bn cyber security
4) BSI UPDATES STANDARDS FOR INFORMATION SECURITY AUDITING
5) HOW TO INTEGRATE SECURITY INTO CORE BUSINESS PROCESSES
6) REBUILDING DIGITAL TRUST IN THE AGE OF THE HACK
7) Celebs, politicos caught in Swiss bank account blackmail
8) BANKING ON SECURITY
9) Cybersecurity experts slam government
10) EUROPEAN COMMISSION PUBLISHES A EUROBAROMETER ON CYBER CRIME

Перечень статей на русском языке для обсуждения с экзаменатором:

1) Импортозамещение и информационная безопасность

2) ИЗ ЧЕГО СКЛАДЫВАЕТСЯ СТОИМОСТЬ DLP-СИСТЕМЫ?
3) КАК НОВЫЕ ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЕВРОСОЮЗЕ ПОВЛИЯЮТ НА ПРЕДПРИЯТИЯ
4) МАШИННОЕ ОБУЧЕНИЕ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ СТАНЕТ ПРИЧИНОЙ ВОЗНИКНОВЕНИЯ БОЛЬШОГО ОБЪЕМА ДАННЫХ, ИНФОРМАЦИИ И РОСТА РАСХОДОВ НА АНАЛИТИКУ
5) Эксперты разработали план по международному противодействию киберпреступности
6) Национальный интернет и отечественное ПО обойдутся госбюджету РФ в 100 млрд рублей
7) НЕБОЛЬШАЯ РЕМАРКА К СТРАТЕГИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ
8) КАСПЕРСКАЯ ВОЗГЛАВИТ ЦЕНТР КОМПЕТЕНЦИЙ ПО ИНФОБЕЗОПАСНОСТИ
9) На подходе ГОСТ по идентификации и аутентификации
10) В России готовят налоговые льготы для компаний, занятых информационной безопасность

Перечень тем по дисциплине для беседы с экзаменатором:

1. The economic aspect of information security
2. National security
3. Information as a product
4. Information resources management
5. Information security in terms of globalization
6. IT risk management systems
7. Corporate management in terms of Information security
8. Efficiency Assessment of the IT systems
9. Digital economy
10. Micro and macro aspects of Digital economy