

Министерство общего и профессионального образования Ростовской области
государственное бюджетное профессиональное образовательное учреждение Ростовской области
«Ростовский-на-Дону колледж связи и информатики»
(ГБПОУ РО «РКСИ»)

ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

по специальности

09.02.03 «Программирование в компьютерных системах»

Студент Воронин Александр Михайлович

(Фамилия, имя, отчество)

Курс 4 Группа ПОКС-49

Общепрофессиональная дисциплина:
ОП.14 «Информационная безопасность»

Преподаватель колледжа:

_____ О.П. Манакова

Студент:

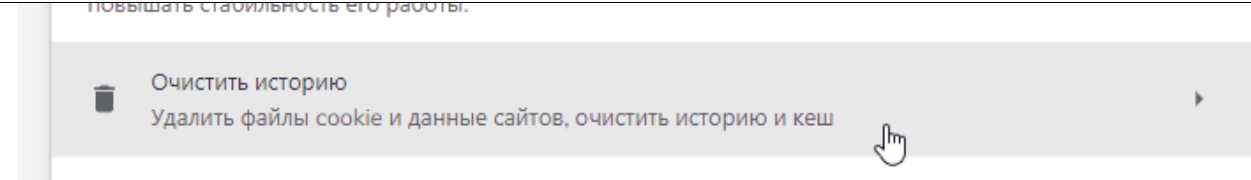
_____ Воронин А.М.

Ростов-на-Дону

2021-2022 уч. г.

Практическое занятие №1

1. Наименование практического занятия: Настройки безопасности и конфиденциальности в браузере.
2. Цели практического занятия: Исследовать настройки безопасности и конфиденциальности в браузере.
3. Количество часов: 2
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: компьютер, выход в глобальную сеть, комплект учебно-методической документации, раздаточный материал, операционная система MS Windows, браузер Google Chrome.
6. Последовательность проведения работ:

№ п/п	Этап выполнения задания	Описание выполняемых работ
1	Очистить кэш и куки в браузере.	

2

Найти сайты требующие работу с куки и проверить их работу (скорость загрузки, правильность отображения контента) при отключенных куки в браузере (интернет-магазины, погода и т.п.).

The image shows two screenshots of the Yandex Market website (market.yandex.ru) with cookie settings disabled in the browser.

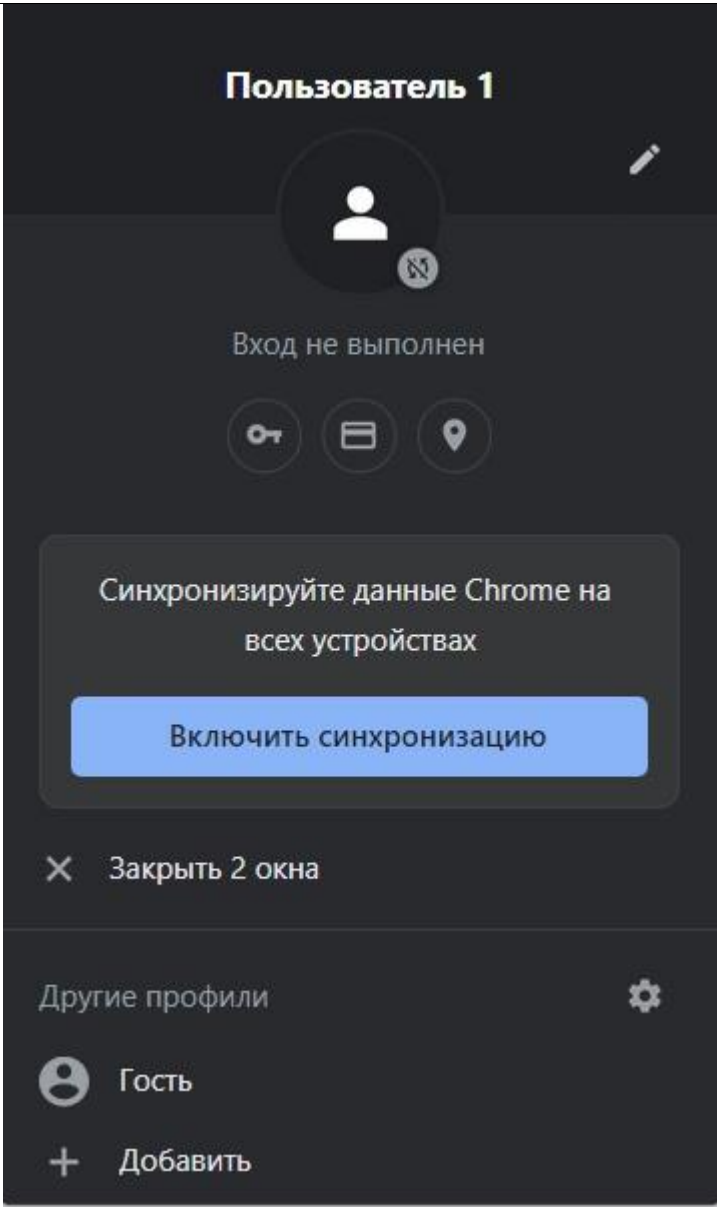
Top Screenshot: The browser's cookie notification bar shows "Используется 87 файлов cookie". The website header features a promotion: "Товары для постного стола со скидкой 35%". The main banner advertises "Желанные подарки со скидками до 80%". Below the banner, the "Электроника и техника для дома" section is visible, with a sub-section for "Общие настройки". The cookie settings are listed as follows:

- ☐ Разрешить все файлы cookie
- ☐ Блокировать сторонние файлы cookie
- ☒ Заблокировать все файлы cookie (не рекомендуется)

Below these settings, there are three informational messages:

- Сайты не могут использовать файлы cookie, чтобы сделать работу в браузере более удобной, например запоминая товары в корзине или информацию о том, что вы вошли в аккаунт
- Сайты не могут использовать файлы cookie, чтобы отслеживать ваши действия в браузере, например, для показа персонализированной рекламы.
- Функции многих сайтов могут стать недоступными

Bottom Screenshot: The browser's cookie notification bar shows "Используется 0 файлов cookie". The website header features a promotion: "и до 20% на цветы для самых любимых". The main banner advertises "Продукты со скидкой на первый заказ - 30%".

3	Выполнить запрет на синхронизацию.	 <p>The screenshot shows the Chrome user profile interface for 'Пользователь 1'. At the top, there is a profile icon with a lock symbol and the text 'Вход не выполнен'. Below this are three circular icons: a key, a wallet, and a location pin. A central notification box prompts the user to 'Синхронизируйте данные Chrome на всех устройствах' with a blue button labeled 'Включить синхронизацию'. At the bottom, there is a section for 'Другие профили' with options for 'Гость' and '+ Добавить'.</p>
---	------------------------------------	---

4	Включить режим инкогнито.	
5	Вернуть начальные настройки браузера.	

6

Проверить наличие цифровых сертификатов, описать назначение 2-3 цифровых сертификатов.

The image displays three screenshots of Russian e-commerce websites, each with a digital certificate overlaid. The certificates are issued by Sectigo RSA Domain Validation Secure Server CA and are valid for the respective domains.

Yandex Market (market.yandex.ru): The certificate is issued to market.yandex.com and is valid from 25.02.2022 to 26.08.2022. The website shows a promotion for Oral-B electric toothbrushes.

Techport.ru: The certificate is issued to *.techport.ru and is valid from 19.12.2021 to 20.12.2022. The website shows a promotion for furniture.

Wildberries (wildberries.ru): The certificate is issued to *.wildberries.ru and is valid from 16.08.2021 to 17.09.2022. The website shows a promotion for clothing.

7. Контрольные вопросы:

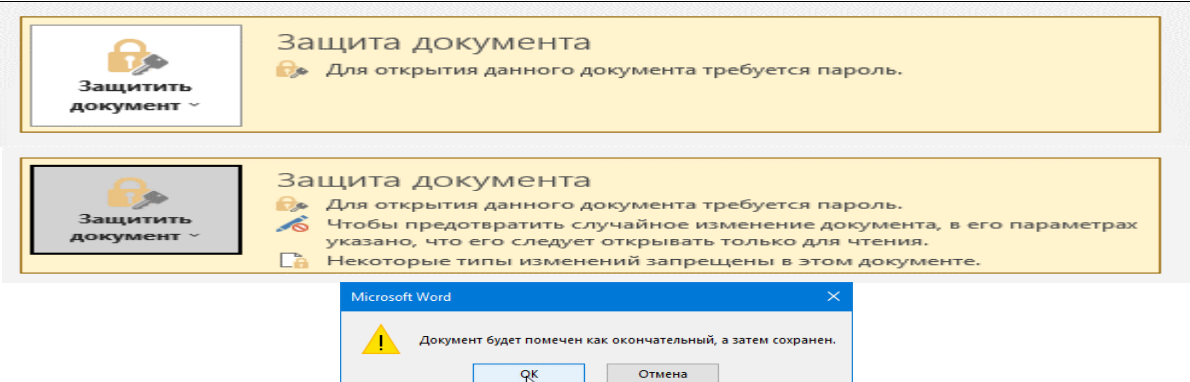
- Всегда ли необходимо отключать файлы куки? Обоснуйте ответ.
Отключать их совсем не стоит, т.к. это будет мешать функционированию сайта. Но они в свою очередь используются для слежки, рекламы, запоминает информацию о ваших посещениях.
- В каких случаях необходимо включать режим инкогнито?
Для большей конфиденциальности, при закрытии режима инкогнито будут сброшены куки и история посещений.

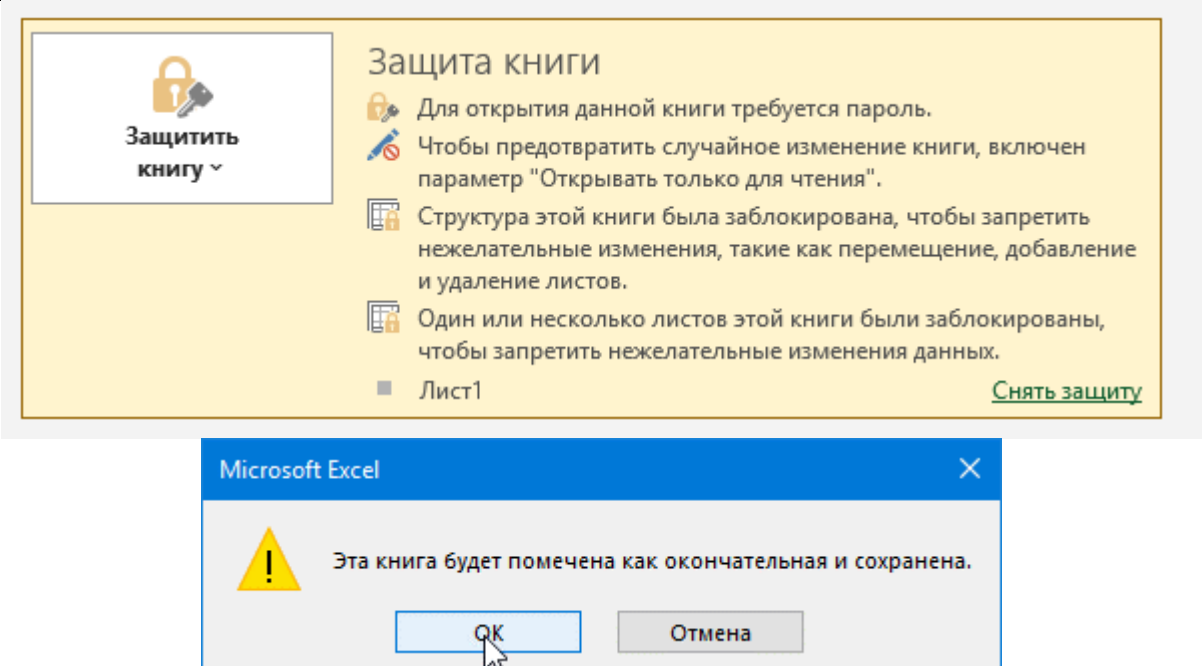
8. Выводы о проделанной работе.

Благодаря данной работе, были закреплены знания пользования куки и режимом инкогнито.

Практическое занятие № 2

1. Наименование практического занятия: Защита документов в MS Office.
2. Цели практического занятия: Исследовать возможности настройки защиты документов в MS Office.
3. Количество часов: 2
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: компьютер, выход в глобальную сеть, комплект учебно-методической документации, раздаточный материал, операционная система MS Windows, MS Office.
6. Последовательность проведения работ:

№ п/п	Этап выполнения задания	Описание выполняемых работ
1	<p>1. В текстовом редакторе MS Word в пункте меню <i>файл</i> → <i>сведения</i> → <i>защитить документ</i> реализовать следующие механизмы защиты:</p> <p>а. Установить пароль на открытие документа.</p> <p>б. Установить ограничение на редактирование «только чтение» для текущего документа.</p>	

	<p>с. Определить произвольные фрагменты документа и группы пользователей, которым разрешено их редактирование.</p> <p>д. Установить защиту на редактирование.</p> <p>е. Пометить документ как окончательный.</p>	
2	<p>1. В текстовом редакторе MS Excel в пункте меню <i>файл</i> → <i>сведения</i> → <i>защитить книгу</i> реализовать следующие механизмы защиты:</p> <p>а. Установить пароль на открытие документа.</p> <p>б. Установить защиту на все листы книги, разрешив только выделение ячеек.</p> <p>с. Выполнить защиту структуры книги.</p> <p>д. Пометить документ как окончательный.</p>	

7. Контрольные вопросы:

1. MS Word. Что подразумевается под опцией «окончательный документ»? Какие действия с ним возможны?

Под подразумевается что документ будет помечен как окончательный, чтобы показать что его редактирование завершено и он является окончательной версией данного документа. При его открытии, будет высвечиваться предупреждение что документ является окончательным, но будет кнопка «все равно редактировать».

2. MS Word. Как снять пароль на документе?

Нужно зайти в Сведения > Защита документа > И выбрать зашифровать документ паролем, после чего стереть заданный пароль и сохранить документ.

3. MS Word. В каком случае опция «зашифровать паролем» будет доступна?

Если будут права на редактирование документа.

4. MS Word. Как отменить защиту на редактирование областей документа?

На вкладке Рецензирование в группе Защитить нажать кнопку Защитить документ и выбрать пункт Ограничить форматирование и редактирование. После в области задач Ограничить форматирование и редактирование нажать кнопку Отключить защиту.

5. MS Excel. Какие действия по защите книги необходимо выполнить, что бы злоумышленник не нарушил ее структуру?

Установить пароль на открытие документа, установить защиту на все листы книги, разрешив только выделение ячеек и выполнить защиту структуры книги.

6. MS Excel. Сможет ли защита элементов листа и книги не допустить компрометации книги? Обоснуйте ответ.

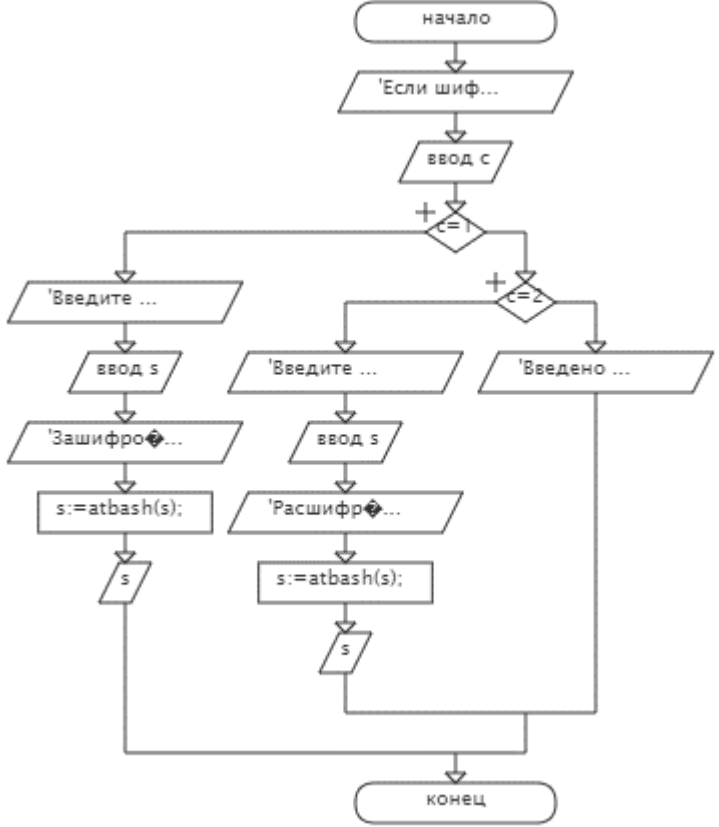
Не вся защита идеальна, и имеет свои уязвимости для злоумышленника.

8. Выводы о проделанной работе.

Благодаря данной работе были закреплены знания по защите документа и книги в таких программах как MS Word и MS Excel.

Практическое занятие № 3

1. Тема практического занятия: Программная реализация алгоритма шифрования и дешифрования информации.
2. Цели практического занятия: Создание программы, реализующей алгоритм шифрования и дешифрования информации.
3. Количество часов: 8
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: компьютер, выход в глобальную сеть, комплект учебно-методической документации, раздаточный материал, операционная система MS Windows, среды программирования.
6. Последовательность проведения работ:

№ п/п	Этап выполнения задания	Описание выполняемых работ
1	Используя знания, умения и навыки, полученные при изучении дисциплины «Технология разработки программного продукта», распределить функции между членами группы, разработать постановку задачи, построить ее блок-схему.	 <pre> graph TD Start([начало]) --> Cond1{Если шиф...} Cond1 --> InputC[/ввод с/] InputC --> LoopStart{+ c=1} LoopStart --> Input1[/Введите .../] Input1 --> InputS1[/ввод s/] InputS1 --> Process1[Зашифро...] Process1 --> Assign1[s:=atbash(s);] Assign1 --> OutputS1[/s/] LoopStart --> LoopEnd{+ c=2} LoopEnd --> Input2[/Введите .../] Input2 --> InputS2[/ввод s/] InputS2 --> Process2[Расшифро...] Process2 --> Assign2[s:=atbash(s);] Assign2 --> OutputS2[/s/] LoopEnd --> Input3[/Введено .../] OutputS1 --> End([КОНЕЦ]) OutputS2 --> End Input3 --> End </pre>

2	Используя любой язык программирования разработать программный продукт.	<pre> const alf='абвгдеёжзийклмнопрстуфхцчшщъыьэюя'; function atbash(s:string):string; var i:integer; begin for i:=1 to Length(s) do s[i]:=alf[33-pos(s[i],alf)+1]; atbash:=s; end; var s:string; var c:integer; begin writeln('Если шифровка введите 1, если дешифровка введите 2'); readln(c); if c=1 then begin writeln('Введите строку для шифрования'); readln(s); writeln('Зашифрованная строка'); s:=atbash(s); writeln(s); end else if c= 2 then begin writeln('Введите строку для дешифрования'); readln(s); writeln('Расшифрованная строка'); s:=atbash(s); writeln(s); end else begin writeln('Введено некоректное число выбора!'); end; end. </pre>
3	Произвести его оптимизацию.	Произведена.
4	Произвести отладку программы.	Произведена.

5	Произвести тестирование программы.	<div>Если шифровка введите 1, если дешифровка введите 2</div> <div>1</div> <div>Введите строку для шифрования</div> <div>арбуз</div> <div>Зашифрованная строка</div> <div>яюлч</div> <hr/> <div>Если шифровка введите 1, если дешифровка введите 2</div> <div>2</div> <div>Введите строку для дешифрования</div> <div>яюлч</div> <div>Расшифрованная строка</div> <div>арбуз</div> <hr/> <div>Если шифровка введите 1, если дешифровка введите 2</div> <div>3</div> <div>Введено некоректное число выбора!</div>
---	------------------------------------	--

7. Контрольные вопросы:

1. Какие языковые конструкции использованы в программе.

Function, цикл for, if then else, writeln, readln.

2. Использовались ли процедуры и функции? Описать их назначение.

Использовалась функция atbash, которая выполняла задачу шифровки и дешифровки. Получая исходный текст, она возвращала зашифрованный или дешифрованный текст.

3. Используя листинг программы, пояснить работу операторов выполняющих ключевые функции программы.

8. Выводы о проделанной работе.

Благодаря данной практической работе, были закреплены навыки владения созданием блок-схем и программного кода.

Практическое занятие № 4

1. Наименование практического занятия: Система информационной безопасности в организации.
2. Цели практического занятия: Построить систему обеспечения информационной безопасности (СОИБ) условной организации, сформировать последовательность этапов построения СОИБ и перечислить мероприятия, реализуемые на каждом из этапов.
3. Количество часов: 8
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: класс ПК, сеть Интернет, операционная система MS Windows, браузеры, MS Office, индивидуальное задание, конспект лекций, комплект учебно-методической документации, электронные и бумажные методические и справочные материалы.
6. Последовательность проведения работ:

Ход занятия (деятельность студентов):

1. Организовать постоянный состав микрогруппы (ФИО участников заявить преподавателю).
2. Выбрать из предложенного списка организацию для реализации индивидуального задания.
3. Ознакомиться с электронными и бумажными методическими и справочными материалами.
4. Реализовать индивидуальное задание в соответствии с поставленными задачами.
5. Оформить полученные результаты в текстовом файле. Сдать на проверку преподавателю.

Список организаций (выбрать одну):

1. Салоны красоты.
2. Автомобили: прокат, аренда.
3. АЗС.
4. Выставки.
5. Строительное оборудование.
6. Кинотеатры.
7. Планетарий (дельфинарий).
8. Туризм.
9. Торговые базы.
10. Бытовые услуги.
11. Изготовление мебели.
12. Гостиница.
13. Издательские услуги.

14. Грузовые перевозки

15. Провайдеры.

Задачи (для любого индивидуального задания):

1. определить цели и задачи защиты информации в организации;
2. составить матрицу доступа;
3. определить группу требований к автоматизированной системе (АС);
4. определить предмет защиты в организации;
5. выявить возможные угрозы защищаемой информации в организации и их структуру;
6. выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в организации;
7. выявить каналы и методы несанкционированного доступа к защищаемой информации в организации;
8. определить основные направления, методы и средства защиты информации в организации.

При составлении файла необходимо придерживаться следующей структуры отчета:

1. Описание организации.
2. Характеристика информационной системы организации.
3. Актуальность проблемы защиты информации в организации.
4. Задачи индивидуального задания.
5. Цели и задачи защиты информации в организации.
6. Матрица доступа.
7. Требования по защите информации от НСД.
8. Объекты и предмет защиты в организации.
9. Угрозы защищаемой информации в организации.
10. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в организации.
11. Каналы и методы несанкционированного доступа к защищаемой информации в организации.
12. Основные направления, методы и средства защиты информации в организации.
13. Выводы.

Критерии оценивания результатов практического занятия.

Результат	Критерии
Зачет	ставится, если студент выполнил работу в полном объеме с соблюдением необходимой последовательности действий; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок. Работа студента характеризуется высокой и средней степенью самостоятельности. Отчет по практическому занятию сдан в установленные сроки.
Не зачет	ставится, если студент выполнил работу не полностью, объем выполненной части таков, что не позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки. Работа студента характеризуется низкой степенью самостоятельности. Отчет по практическому занятию не сдан в установленные сроки.

Выполнение практической работы

Состав микрогруппы: Студент ПОКС-49 Воронин А.М.
Туризм «Travelcart»

Бизнес-трелвел агентство Travelcart более двадцати лет успешно работает в сфере туризма. Оперативность, качественное оказание услуг и персональная забота о путешественнике — наши главные приоритеты. Мы состоим в Международной ассоциации авиаперевозчиков (IATA), что позволяет осуществлять взаиморасчеты через удобную и современную систему BSP. Помимо этого, мы являемся членами Единого Федерального реестра туроператоров и ассоциации «Турпомощь». Наше агентство тесно сотрудничает с лучшими страховыми компаниями России. При этом мы хорошо знаем все нюансы оформления страховых полисов всех типов — это дает нашим клиентам гарантию получения возмещения в случае возникновения непредвиденных обстоятельств.

В штате Travelcart работает собственная группа IT-разработчиков, благодаря которой создаются и постоянно модернизируются онлайн-проекты. Профессиональные менеджеры нашей компании найдут подход к каждому клиенту и готовы прийти на помощь в любой момент.

Информационные процессы, происходящие повсеместно в нашей организации, выдвигают на первый план, наряду с задачами эффективного обработки и передача информации, важнейшую задачу обеспечения безопасности

информации. Это объясняется особой значимости для развития «Travelcart» его информационных ресурсов, ростом стоимости информации, её высокой уязвимостью и нередко значительным ущербом в результате ее несанкционированного использования.

Цель технической защиты информации - обеспечение целостности, конфиденциальности и доступности защищаемой информации в нашей организации. Основные задачи технической защиты информации: предотвращение утечки информации через технические каналы утечки информации; предотвращение несанкционированного доступа к информации нашей организации «Travelcart».

Документ	Субъект	Чтение	Изменение	Исполнение	Просмотр	Удаление	Полный доступ
Сведения о клиентах	Начальник	+	+	+	+	+	+
Сведения о клиентах	Бухгалтер	+	-	+	+	-	-
Сведения о клиентах	Сотрудник	+	+	+	+	-	-
Расписание маршрутов	Начальник	+	+	+	+	+	+
Расписание маршрутов	Бухгалтер	+	-	-	+	-	-
Расписание маршрутов	Сотрудник	+	-	+	+	-	-
План техосмотра автобусов	Начальник	+	+	+	+	+	+
План техосмотра автобусов	Бухгалтер	+	-	-	+	-	-
План техосмотра автобусов	Сотрудник	-	-	-	-	-	-

Таблица 1 – Матрица доступа

Непосредственно предметом защиты организации будут база данных наших клиентов, а также безопасного подключения в конференции между сотрудниками организации. Существуют такие угрозы для базы данных как:

1. Неограниченные привилегии базы данных

Это действие может быть совершено как действующими, так и бывшими сотрудниками компании.

2. Внедрение SQL-кода

Целью этого всего обычно является кража данных или их повреждение. Внедрение SQL-кода нацелено на традиционные базы данных, а Внедрение NoSQL кода - на базы BIG Data

3. Плохой аудиторный след

Согласно некоторым стандартам безопасности, каждое событие в базе данных должно быть записано для целей аудита. Если вы не можете представить доказательства наличия журнала аудита базы данных, то

это может представлять собой очень серьезный риск для безопасности, поскольку в случае вторжения невозможно будет провести расследование.

4. Открытые резервные копии баз данных

Шифрование и аудит производственных баз данных и резервных копий - лучшая форма защиты корпоративных конфиденциальных данных.

5. Неправильная конфигурации базы данных

Это тревожный сигнал, что при настройке базы данных не должно быть ничего похожего на учетную запись по умолчанию, а параметры должны быть настроены таким образом, чтобы злоумышленнику было сложно что-либо сделать.

6. Отсутствие опыта в области безопасности

Сотрудникам службы безопасности может не хватать знаний, необходимых для внедрения средств контроля безопасности и других политик безопасности.

7. Отказ в обслуживании (DoS)

Например, если есть запрос на очень важные финансовые данные, а база данных недоступна из-за DoS, то это может привести к потере денег.

8. Плохое управление данными

Некоторые корпоративные организации не умеют правильно управлять своими конфиденциальными данными, они не ведут их точную инвентаризацию, и таким образом некоторые из этих конфиденциальных данных могут попасть в чужие руки. Если не провести надлежащую инвентаризацию новых данных, добавленных в базу, то они могут стать уязвимыми.

Для решения большинства вышестоящих проблем, мы проводим тестирование безопасности базы данных. Он проводится для обнаружения любых слабых мест или уязвимостей в конфигурации безопасности БД и для смягчения последствий любого нежелательного доступа к базе данных. Все конфиденциальные данные должны быть защищены от злоумышленников, поэтому регулярные проверки безопасности очень важны и обязательны.

Это тестирование должно проводиться на самом раннем этапе жизненного цикла разработки программного обеспечения, чтобы иметь представление об уязвимостях, существующих в системе баз данных, а использование некоторых из этих инструментов поможет обнаружить их эффективно и действенно.

К источникам дестабилизирующего воздействия на информацию относятся : люди; технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи и системы обеспечения их функционирования; природные явления.

Виды и способы дестабилизирующего воздействия на защищаемую информацию дифференцируются по источникам воздействия. Самое большее количество видов и способов дестабилизирующего воздействия имеет отношение к людям. Со стороны людей возможны следующие виды воздействия, приводящие к уничтожению, искажению и блокированию в нашей организации:

1. Непосредственное воздействие на носители защищаемой информации.

Метод решения: установка камер слежения в офисах и перестановка оборудования таким образом, чтобы сложнее было повлиять на носители.

2. Несанкционированное распространение конфиденциальной информации.

Метод решения: разработать способы наказания для подобного рода случаев, включая штрафы и увольнения. Сузить круг сотрудников, способных обладать ценной информацией.

3. Вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.

Метод решения: нанять сотрудника, который будет способен оперативно возобновлять работу оборудования, и пытаться минимизировать такие сбои правильной проводкой и заземлением.

4. Нарушение режима работы перечисленных средств и технологии обработки информации.

Метод решения: разработать график и разделить рабочую среду на кластеры, которые можно будет выключать по заранее разработанному графику.

Также к защите информации от несанкционированного доступа, мы разработали следующие требования:

- Защита Системы должна обеспечиваться комплексом программно-технических средств и поддерживающих их организационных мер.
- Защита Системы должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.
- Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики Системы (надежность, быстродействие, возможность изменения конфигурации).
- Разграничение прав доступа пользователей и администраторов.

7. Контрольные вопросы:

- Какие нормативные документы использовались при построении СОИБ?
- Является ли процедура построения СОИБ циклической? Обоснуйте Ваш ответ.

По-моему мнению да, потому что с каждым разом появляются разные технологии, которые нуждаются в защите от новых видов атак. И стоять на месте просто невозможно.

- Дайте характеристику современным злоумышленникам, совершающим правонарушения в сфере информационной безопасности.

Мастерство и знания мошенника позволяют ему действовать на уровне разработчика, он способен выбрать самое уязвимое место в системе и свободно проникнуть к информации, стать угрозой для неё.

- Обоснуйте необходимость проведения регулярной работы с сотрудниками организации.

Регулярная работа с сотрудниками нужна в первую очередь для того, чтобы не пускать их на самотёк, а держать так сказать «в узде» и контролировать ситуацию информационной безопасности.

- Какова конечная цель полученной СОИБ?

Минимизировать нарушение условий информационной безопасности в организации.

8. Выводы о проделанной работе.

Выполнив данное практическое задание, были получены знания по работе с СОИБ и закреплены знания в сфере информационной безопасности.