Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
О.В. Фомичева
«26» декабря 2023 г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

по текущему контролю успеваемости
и промежуточной аттестации
по учебной дисциплине
ОП.02 ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

программы подготовки специалистов среднего звена

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Санкт-Петербург
2023 г.

Комплект контрольно-оценочных средств по учебной дисциплине разработан на основе Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки России от 09.12.2016 № 1553, в соответствии с рабочей программой учебной дисциплины ОП.02 Организационно-правовое обеспечение информационной безопасности.

Комплект контрольно-оценочных средств рассмотрен на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Комплект контрольно-оценочных средств одобрен на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий
Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

1. ПАСПОРТ КОМПЛЕКТА ОЦЕНОЧНЫХ СРЕДСТВ

В результате освоения учебной дисциплины «Организационно-правовое обеспечение информационной безопасности», обучающийся должен обладать следующими умениями, знаниями, которые формируют профессиональные и общие компетенции:

уметь:

– использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;

– *разрабатывать локальные акты предприятия в области организации защиты коммерческой тайны;*

– *разрабатывать локальные акты предприятия в области защиты персональных данных;*

– *проводить аудит состояния информационной безопасности предприятия*

знать:

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– правовые основы защиты конфиденциальной информации по видам тайны;

– порядок лицензирования деятельности по технической защите конфиденциальной информации;

– правовые основы деятельности подразделений защиты информации;

– правовую основу допуска и доступа персонала к защищаемым сведениям;

– правовое регулирование взаимоотношений администрации и персонала в области защиты информации; систему правовой ответственности за утечку информации и утрату носителей информации;

– правовые нормы в области защиты интеллектуальной собственности;

– порядок отнесения информации к разряду конфиденциальной информации;

– *порядок организации защиты коммерческой тайны на предприятии;*

– *порядок организации защиты персональных данных на предприятии;*

– *структуру политики безопасности предприятия;*

– *порядок проведения аудита информационной безопасности предприятия.*

общие компетенции:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

профессиональные компетенции:

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

Формой **промежуточной аттестации** по учебной дисциплине является экзамен.

Текущий контроль освоения обучающимися программного материала учебной дисциплины проводится с целью объективной оценки качества освоения программы учебной дисциплины, а также стимулирования учебной работы обучающихся, мониторинга результатов образовательной деятельности, подготовки к промежуточной аттестации и обеспечения максимальной эффективности учебно-воспитательного процесса.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих компетенций.

Контроль и оценка результатов освоения дисциплины

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения	
У1 использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; У2 разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации; У3 разрабатывать локальные акты предприятия в области организации защиты коммерческой тайны; У4 разрабатывать локальные акты предприятия в области защиты персональных данных; У5 проводить аудит состояния информационной безопасности предприятия	Оценка практических работ Устные ответы на экзамене
Знания	
З1основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; З2 правовые основы защиты конфиденциальной информации по видам тайны; З3 порядок лицензирования деятельности по технической защите конфиденциальной информации; З4 правовые основы деятельности подразделений защиты информации; З5 правовую основу допуска и доступа	Оценка ответов на устных зачетах Устные ответы на экзамене

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
персонала к защищаемым сведениям; З6 правовое регулирование взаимоотношений администрации и персонала в области защиты информации; систему правовой ответственности за утечку информации и утрату носителей информации; З7 правовые нормы в области защиты интеллектуальной собственности; З8 порядок отнесения информации к разряду конфиденциальной информации; З9 порядок организации защиты коммерческой тайны на предприятии; З10 порядок организации защиты персональных данных на предприятии; З11 структуру политики безопасности предприятия; З12 порядок проведения аудита информационной безопасности предприятия.	

3. ОЦЕНКА ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Текущий контроль. Задания для текущей аттестации

Проводится преподавателем на учебных занятиях, согласно календарно-тематическому плану. Формы текущего контроля выбраны, исходя из методической целесообразности.

Распределение контрольных точек по дисциплине

Дидактические единицы	Проверяемые ОК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 1. Основные нормативно-правовые акты, регламентирующие организацию архивного дела	ОК 1-2, 4, 5, 8, 11, 12 У1, ПК 2.1, ПК 2.9.	Практическая работа № 1. Разработка перечня данных предприятия, составляющих коммерческую тайну.	Ответы на вопросы дифференцированного зачета
	ОК 1, ОК 11, ОК 12 З1, З2	Устный зачет по Теме 1	
Тема 2. Организация защиты персональных данных	ОК 1-2, 4, 5, 8, 11, 12 У2, ПК 2.1	Практическая работа № 5. Разработка положения о защите персональных данных	
	ОК 1, ОК 11, ОК 12 З1, З2	Устный зачет по Теме 2	
Тема 3. Политика безопасности предприятия	ОК 1-2, 4, 5, 8, 11, 12 У3, ПК 2.1, ПК 2.9.	Практическая работа № 8. Разработка концепции информационной безопасности предприятия	
	ОК 1, ОК 11, ОК 12 З1, З2, З3	Устный зачет по Теме 3	
Тема 4. Аудит информационной безопасности предприятия	ОК 1-2, 4, 5, 8, 9, 11, 12 У4, ПК 2.9.	Практическая работа № 10. Проведение аудита состояния информационной безопасности предприятия	
	ОК 1, ОК 11, ОК 12 З1, З2, З3	Устный зачет по Теме 4	

1. Практическая работа № 1. Разработка перечня данных предприятия, составляющих коммерческую тайну

Инструкция для обучающихся
Внимательно прочитайте задание. Разработайте проект перечня данных предприятия, составляющих коммерческую тайну.

Время выполнения задания – 90 минут.

Задание

1. Используя примерный перечень документов, отнесённых к коммерческой тайне, разработайте проект перечня данных предприятия, составляющих коммерческую тайну на предприятии
2. При разработке проекта отредактируйте текст положения с учетом особенностей Вашей организации.
3. Оформление проекта положения должно соответствовать требованиям ГОСТ 7.0.97-2016.

Текст ГОСТа можно прочитать здесь:

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Пример перечня конфиденциальных данных
Перечень сведений, отнесенных к конфиденциальной (служебной) информации в центральном аппарате Федерального агентства железнодорожного транспорта и подведомственных ему предприятиях, и учреждениях, утв. Приказом Федерального агентства железнодорожного транспорта от 24.01.2011 N 18

N п/п	Сведения, отнесенные к конфиденциальной (служебной) информации
I. Сведения об отраслевой управленческой деятельности	
1	Отдельные материалы заседаний Федерального агентства железнодорожного транспорта (далее - Росжелдора) и сведения, содержащиеся в них, ограничение доступа к которым установлено решением заседания ПДТК Росжелдора
2	Сведения (информация), подготовленные Росжелдором на поступающие из органов государственной власти, предприятий, учреждений и организаций, независимо от организационно-правовой формы и формы собственности с пометкой "Для служебного пользования", "Коммерческая тайна", "Конфиденциально" и другие в части, не содержащей сведений, составляющих государственную тайну
3	Сведения, содержащие показатели государственного оборонного заказа в части, не содержащей сведений, составляющих государственную тайну
4	Сведения, содержащиеся в материалах служебной

	проверки (расследования), до утверждения акта (заключения) по проверке, а также если сведения, полученные в результате проверки (расследования), могут быть использованы в дальнейшем для противоправного действия (нанесения ущерба)
5	Сведения об организации работы, о конкретных мерах или проводимых мероприятиях, направленных на обеспечение информационной безопасности при осуществлении международного сотрудничества с участием представителей Росжелдора, а также содержащиеся в подготовительных или отчетных документах (формах) о проведении встречи
II. Сведения об административно-хозяйственной деятельности	
6	Сведения о персональных данных работника Росжелдора, содержащиеся в личном деле работника, кроме случаев, предусмотренных законодательством Российской Федерации
7	Сведения, получаемые при приеме гражданина на государственную гражданскую службу, необходимые для оформления допуска к государственной тайне
8	Сведения об осведомленности работника со сведениями, составляющими государственную тайну
9	Протоколы заседаний конкурсных комиссий по проведению конкурсов на замещение вакантных должностей государственной гражданской службы
10	Акты проверок деятельности территориальных управлений и подведомственных организаций
11	Сведения о штатном расписании Росжелдора
12	Сведения о расположении структурных подразделений в здании
13	Протоколы заседаний жилищной комиссии
14	Протоколы заседаний конкурсной комиссии по проведению квалификационного экзамена и аттестации
III. Сведения о режиме секретности, мобилизационной подготовке, гражданской обороне, чрезвычайных ситуациях и транспортной безопасности	
15	Акты проверок обеспечения пропускного режима в административное здание Росжелдора

16	Сведения о результатах оценки уязвимости объектов транспортной инфраструктуры и транспортных средств, кроме тех, обеспечение безопасности которых осуществляется исключительно федеральными органами исполнительной власти
17	Сведения, содержащиеся в планах обеспечения транспортной безопасности объекта транспортной инфраструктуры и транспортного средства
18	Сведения, являющиеся информационными ресурсами единой государственной информационной системы обеспечения транспортной безопасности, подготовленные Росжелдором, за исключением выписок из реестра категорированных объектов транспортной инфраструктуры и транспортных средств
IV. Сведения о защите информации	
19	Сведения об организации обработки служебной информации на средствах вычислительной техники Росжелдора
20	Сведения, раскрывающие организацию, состояние защиты информации, или носителей информации, или информационного процесса
21	Сведения о методах, средствах или эффективности (состоянии защиты) конфиденциальной информации в автоматизированных информационных системах, средствах вычислительной техники, других технических средствах
22	Обобщенные сведения, содержащиеся в схеме локальной вычислительной сети Росжелдора, с указанием организационно-технологических параметров или технических характеристик и мест расположения ее ответственных составных частей, информационных узлов (определены на схеме)
23	Сведения о конкретных проводимых и (или) планируемых мероприятиях по информационной безопасности конфиденциальной информации
V. Прочие сведения	
24	Сведения об организации, состоянии или расположении инженерных систем видеонаблюдения, пожарной или охранной сигнализации здания Росжелдора
25	Сведения, раскрывающие содержание планов и конкретных мероприятий по

	охране здания Росжелдора, помещений, в которых выполняются работы, хранятся материалы, ведутся переговоры конфиденциального характера
26	Данные охранного видеонаблюдения, фиксации системы охраны помещений, электронной системы прохода в здание

Вставьте ниже разработанный проект

Эталон ответа:

ПЕРЕЧЕНЬ ДОКУМЕНТОВ, ОТНЕСЕННЫХ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
ООО «ГАРАНТ»

К документам, содержащим информацию, составляющую коммерческую тайну ООО «ГАРАНТ» (далее - Организация), отнесены следующие документы:

1. Бизнес-планы, документы о финансовых рисках и прогнозных оценках.
2. Первичные бухгалтерские документы и промежуточные финансовые отчеты Организации.
3. Регистры бухгалтерского учета, внутренняя бухгалтерская отчетность Организации.
4. Договоры, контракты и соглашения Организации, а также сведения об их исполнении.
5. Отчеты о реализации продукции, закупаемой (производимой) Организацией, отчеты о продажах.
6. Результаты научных исследований и проектных разработок, выполненных работниками Организации или сторонними компаниями по соглашению с организацией.
7. Документы, содержащие сведения о получаемых и предлагаемых заказах и предложениях.
8. Документы по организации и проведению конкурсов (торгов).
9. Деловая переписка.
10. Документы о подготовке и ведении переговоров.
11. Протоколы закрытых совещаний и переговоров.
12. Документы, содержащие сведения о лицах, ведущих переговоры, руководстве сторонних компаний, их характеристика.
13. Материалы и приложения, получаемые/передаваемые в процессе проведения переговоров.
14. Кадровое делопроизводство.
15. Образцы подписей работников Организации.
16. Штатное расписание Организации.
16.1. Персональные данные работников.
16.2. Документы, содержащие информацию о системе охраны в Организации.
16.3. Документы, содержание информацию о пропускном режиме в Организации.
16.4. Пропуска и удостоверения работников Организации.

2. Устный зачет по Теме 1

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Назовите основные нормативно- правовые и методические документы в области архивного дела в РФ. Дайте их краткую характеристику.
2. Охарактеризуйте структуру управления архивным делом в РФ.
3. Дайте определение понятия АФ РФ. Назовите документы, входящие в состав АФ РФ.
4. Как осуществляется учет документов, входящих в состав АФ РФ?
5. Какова процедура комплектования архивов архивными документами?
6. Какие существуют ограничения на доступ к архивным документам?
7. При каких условиях возможен вывоз архивных документов за пределы РФ?
8. Дайте определение понятия «архив», перечислите виды архивов.
9. Перечислите функции архива организации.
10. Охарактеризуйте порядок разработки, оформления, согласования и утверждения Положения об архиве организации.

Эталоны ответов: приведены в Учебном пособии по дисциплине «Правовое обеспечение информационной информации».

3. Практическая работа № 5. Разработка положения о защите персональных данных

Инструкция для обучающихся

Внимательно прочитайте задание. Разработайте положение о защите персональных данных.

Время выполнения задания – 60 минут.

Задание

1. Создайте или найдите в сети Интернет и адаптируйте под свою организацию проект «Положение о защите персональных данных»
2. При разработке проекта отредактируйте текст положения с учетом особенностей Вашей организации.
3. Оформление проекта положения должно соответствовать требованиям ГОСТ 7.0.97-2016.

Текст ГОСТа можно прочитать здесь:

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Варианты

Номер варианта	Организация

1	Отделение коммерческого банка
2	Поликлиника
3	Колледж
4	Офис страховой компании
5	Рекрутинговое агентство
6	Интернет-магазин
7	Центр оказания государственных услуг
8	Отделение полиции
9	Аудиторская компания
10	Дизайнерская фирма
11	Офис интернет-провайдера
12	Офис адвоката
13	Компания по разработке ПО для сторонних организаций
14	Агентство недвижимости
15	Туристическое агентство
16	Офис благотворительного фонда
17	Издательство
18	Консалтинговая фирма
19	Рекламное агентство
20	Отделение налоговой службы
21	Офис нотариуса
22	Бюро перевода (документов)
23	Научно проектное предприятие
24	Брачное агентство
25	Редакция газеты
26	Гостиница
27	Праздничное агентство
28	Городской архив
29	Диспетчерская служба такси
30	Комплексный центр социального обслуживания населения

Эталон ответа:

УТВЕРЖДЕНО
Приказом директора
ЗАО «КЦСОН»
от 10.01.2017 г. № 01-о

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников закрытого акционерного общества «Комплексный центр социального обслуживания населения»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников закрытого акционерного общества «Комплексный центр социального обслуживания населения» (далее – ЗАО «КЦСОН», Учреждение, Работодатель). Под работниками подразумеваются лица, заключившие трудовой договор с Учреждением.

1.2. Обработка персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, защиты персональных данных работников Учреждения от несанкционированного доступа и разглашения. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

1.3. Основанием для разработки настоящего Положения являются Конституция Российской Федерации, Трудовой кодекс Российской Федерации, другие действующие нормативные правовые акты Российской Федерации.

1.4. Настоящее Положение и изменения к нему утверждаются директором Учреждения и вводятся приказом по Учреждению. Все работники Учреждения должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

2. ОСНОВНЫЕ ПОНЯТИЯ. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

2.1. Для целей настоящего Положения используются следующие основные понятия:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (п. 1 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

обработка персональных данных работника - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (п. 3 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

распространение персональных данных - действия, направленные на раскрытие персональных данных работников неопределенному кругу лиц (п. 5 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

предоставление персональных данных - действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц (п. 6 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

блокирование персональных данных - временное прекращение обработки персональных данных работников (за исключением случаев, если обработка необходима для уточнения персональных данных) (п. 7 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников (п. 8 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику (п. 9 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ).

2.2. Если иное не установлено Трудовым кодексом РФ, другими федеральными законами, при заключении трудового договора лицо, поступающее на работу, предъявляет работодателю:

паспорт или иной документ, удостоверяющий личность;

трудовую книжку, за исключением случаев, когда договор заключается впервые, или работник поступает на работу на условиях совместительства, или трудовая книжка у работника отсутствует в связи с ее утратой, повреждением или по другим причинам;

страховое свидетельство обязательного пенсионного страхования;

документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;

документ об образовании и (или) квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

документы о прохождении предварительного медицинского осмотра при поступлении на работу и периодических медицинских осмотров, в период действия трудовых отношений;

дополнительные документы - в отдельных случаях, предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента РФ и постановлениями Правительства РФ;

согласие на обработку персональных данных (приложение 1 к настоящему Положению).

2.3. Состав персональных данных работника:

- фамилия, имя, отчество,
- год, месяц, дата, место рождения;
- гражданство;
- образование;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- специальность;
- занимаемая должность;
- адрес места жительства;
- домашний телефон.

2.4. В Учреждении создаются и хранятся следующие группы кадровых документов, содержащие данные о работниках в единичном или сводном виде:

2.4.1. Документы, содержащие персональные данные работников:

комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

подлинники и копии приказов (распоряжений) по кадрам;

личные дела и трудовые книжки;

- основания к приказам по личному составу;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным работника;
- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

2.5. Данные документы являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

3. ОБЯЗАННОСТИ РАБОТОДАТЕЛЯ

3.1. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.1.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.1.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

3.1.3. Все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.1.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.1.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.1.6. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.1.7. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

3.1.8. Работники и их представители должны быть ознакомлены под роспись с документами предприятия, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.1.9. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

4. ОБЯЗАННОСТИ РАБОТНИКА

Работник обязан:

4.1. Передавать работодателю или его представителю комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом Российской Федерации.

4.2. Своевременно в разумный срок, не превышающий 5 дней, сообщать работодателю об изменении своих персональных данных.

4.3. Работник, осуществляющий обработку персональных данных, обязан подписать обязательство о соблюдении конфиденциальности персональных данных (приложение 2 к настоящему Положению).

5. ПРАВА РАБОТНИКА

Работник имеет право:

5.1. На полную информацию о своих персональных данных и обработке этих данных.

5.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством Российской Федерации.

5.3. На доступ к медицинским данным с помощью медицинского специалиста по своему выбору.

5.4. Требовать исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных трудовым законодательством. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.5. Требовать извещения работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.6. Обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите его персональных данных.

5.7. Определять своих представителей для защиты своих персональных данных.

6. СБОР, ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных работника - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных работника.

6.2. Все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

6.3. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

6.4. Работник представляет работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами. Представление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

6.5. Личное дело работника оформляется после издания приказа о приеме на работу.

6.5.1. Все документы личного дела подшиваются в обложку образца, установленного на предприятии. На ней указываются фамилия, имя, отчество работника, номер личного дела.

6.5.2. Все документы, поступающие в личное дело, располагаются в хронологическом порядке. Листы документов, подшитых в личное дело, нумеруются.

6.5.3. Личное дело ведется на протяжении всей трудовой деятельности работника. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

7. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

8. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКА

8.1. Внутренний доступ (доступ внутри Учреждения).

Право доступа к персональным данным работника имеют:

- директор Учреждения;
- специалист отдела кадров;
- заведующие отделениями (доступ к личным данным только работников своего отделения) по согласованию с директором Учреждения;
- сотрудники бухгалтерии - к тем данным, которые необходимы для выполнения конкретных функций;
- сам работник, носитель данных.

8.2. Внешний доступ.

Персональные данные вне организации могут представляться в государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

8.3. Другие организации.

Сведения о работнике (в том числе уволенном) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

9. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

9.1. В целях обеспечения сохранности и конфиденциальности персональных данных работников Учреждения все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только специалистом отдела кадров, осуществляющим данную работу в соответствии со своими служебными обязанностями, зафиксированными в его должностной инструкции.

9.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке предприятия и в том объеме, который позволяет не разглашать излишний объем персональных сведений о работниках Учреждения.

9.3. Передача информации, содержащей сведения о персональных данных работников организации, по телефону, факсу, электронной почте без письменного согласия работника запрещается.

9.4. Личные дела и документы, содержащие персональные данные работников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

9.5. Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РАБОТНИКА

10.1. Лица, виновные в нарушении положений законодательства РФ в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

10.2. Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, установленных Федеральным законом от 27.07.2006 N 152-ФЗ, подлежит возмещению в соответствии с законодательством РФ. Возмещение

морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

4. Устный зачет по Теме 2

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Что такое персональные данные?
2. На основании, каких документов составляется перечень ПДн?
3. Перечислите все категории ПДн.
4. Какими критериями служат для определения категории ПДн?
5. На основании, каких документов определяется перечень сотрудников, обрабатывающих ПДн?
6. Что такое класс информационной системы обработки ПДн?
7. Опишите методику определения класса информационной системы обработки ПДн.
8. Назовите основные организационные меры, которые используются для защиты ПДн.
9. Назовите основные виды программных и программно-аппаратных средств, использующихся при защите ПДн.

Эталоны ответов: приведены в Учебном пособии по дисциплине «Правовое обеспечение информационной безопасности».

5. Практическая работа № 8. Разработка концепции информационной безопасности предприятия

Инструкция для обучающихся

Внимательно прочитайте задание. Разработайте концепцию информационной безопасности предприятия.

Время выполнения задания – 60 минут.

Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.

- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы.

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия.
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

Варианты

Номер варианта	Организация
1	Отделение коммерческого банка
2	Поликлиника
3	Колледж
4	Офис страховой компании
5	Рекрутинговое агентство
6	Интернет-магазин
7	Центр оказания государственных услуг
8	Отделение полиции
9	Аудиторская компания
10	Дизайнерская фирма
11	Офис интернет-провайдера
12	Офис адвоката
13	Компания по разработке ПО для сторонних организаций
14	Агентство недвижимости
15	Туристическое агентство
16	Офис благотворительного фонда

17	Издательство
18	Консалтинговая фирма
19	Рекламное агентство
20	Отделение налоговой службы
21	Офис нотариуса
22	Бюро перевода (документов)
23	Научно проектное предприятие
24	Брачное агентство
25	Редакция газеты
26	Гостиница
27	Праздничное агентство
28	Городской архив
29	Диспетчерская служба такси
30	Комплексный центр социального обслуживания населения

Эталон ответа:

" У Т В Е Р Ж Д А Ю "
Генеральный директор
ЗАО «КЦСОН»

_____Козлов А.И.
"26" апреля 2017г.

Концепция информационной безопасности
Закрытого акционерного общества «Комплексный центр социального обслуживания населения»

Настоящий документ определяет цели, политику в области защиты информации, обозначает задачи, принципы и основные пути обеспечения информационной безопасности (ИБ) ЗАО «КЦСОН». Концепция является *базовым нормативно-информационным документом* и служит основой для:

- создания единой системы правовых, организационных, технических, режимных и иных мер, обеспечивающих защищенность ЗАО «КЦСОН» в информационной сфере;
- разработки программ и мероприятий по обеспечению информационной безопасности ЗАО «КЦСОН», подготовки локальных нормативных документов и политик.

Организация системы ИБ.

- Генеральный директор – определяет направления и меры по реализации *Концепции информационной безопасности*;
- Совет директоров и Генеральный директор – предусматривают выделение средств и координируют работу подразделений по вопросам ИБ;
- ИТ-директор – обеспечивает выполнение технических мер ИБ компании, подбор лучших практик и их внедрение, подготовку локальных документов и политик;
- Руководители подразделений – обеспечивают выполнение всеми подчиненными сотрудниками установленных требований ИБ;
- обеспечение ИБ непосредственно на рабочих местах возлагается на сотрудников подразделений.

Ответственность за нарушение требований ИБ. По степени опасности нарушения ИБ делятся на две группы:

- нарушения, повлекшие за собой наступление нежелательных для компании последствий (*утечку или уничтожение информации*);

- нарушения, создавшие предпосылки нежелательных для компании последствий (*угроза уничтожения или утраты информации*).

Нарушение требований локальных нормативных документов по ИБ является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, локальными нормативными актами и договорами, заключенными между компанией и сотрудниками. Степень ответственности за нарушение требований локальных нормативных актов в области ИБ определяется исходя из размера ущерба, причиненного компании. Руководители структурных подразделений компании несут персональную ответственность за обеспечение ИБ в возглавляемых ими подразделениях.

Настоящий документ - *Концепция информационной безопасности* - обязателен для ознакомления руководителями всех структурных подразделений компании.

I. ВВЕДЕНИЕ

Информационная безопасность (ИБ) есть защищенность, сохранность информационных ресурсов от случайных, злонамеренных или чрезвычайных внутренних/внешних воздействий и сбоев.

Общая ***задача ИБ*** состоит в минимизации ущерба, в предсказании и непрерывном предотвращении таких воздействий. ИБ, как важная компонента обеспечения устойчивости бизнеса, *обеспечивается* комплексом организационных, технологических и технических решений и систем. Основы видения и политика ИБ обозначаются настоящим документом, а именно:

- цели и пути создания системы защиты;
- объекты защиты и их характеристика;
- анализ рисков, описывающий финансовые потери, ущерб и потери по другим критериям;
- основные классы и источники угроз ИБ; вероятность угроз и уязвимость ресурсов;
- основные принципы и подходы к построению системы обеспечения ИБ, методы и средства.

II. ЦЕЛИ И ЗАДАЧИ

Целью системы защиты является обеспечение бесперебойной работы аппаратно-программных средств компании, непрерывная поддержка бизнес-процессов и документооборота, сохранность и достоверность информационных ресурсов, их защищенность от внутренних/внешних воздействий, а также при чрезвычайных обстоятельствах.

Пути достижения целей можно выделить в несколько обязательных направлений:

1. Организационно-административные мероприятия и регламенты:

- *определение ответственности* за работоспособность и сохранность ресурсов компании четырех групп сотрудников: **а)** руководителей компании за выделение средств на приобретение, развертывание систем, обучение специалистов, развитие и пр.; **б)** ИТ-специалистов за оперативное обеспечение работоспособности и управление ИТ; **в)** конечных пользователей; **г)** сотрудников охраны;
- *определение статуса ИТ*, как сервисно-технологического подразделения, предоставляющего услуги, и статуса других подразделений – потребителей услуг;
- *обязательное планирование* развития информационных ресурсов, технологий и защиты, для достижения устойчивости бизнеса и долговременных конкурентных преимуществ;

- *централизация* в ИТ-подразделении всех мероприятий и бюджетов по закупке, установке аппаратных и программных средств, работе с любыми внешними поставщиками ИТ-услуг;
- *выработка политик* пользования информационно-технологическими ресурсами, политик поддержки пользователей, политик на ИТ-работы (производственные, проектные, для экстренных ситуаций), других правовых норм и ответственности по ИБ для всех групп сотрудников (при приеме на работу, на период работы);
- *контроль доступа пользователей* к ИТ-ресурсам компании – принятие на работу и увольнение сотрудников с обязательным прохождением через ИТ-подразделение (собеседование, квалификация и пр.).

2. Надежность, живучесть, достоверность аппаратного и программного обеспечения:

- *закупка* оборудования и программного обеспечения только известных производителей и продавцов; использование лицензионного программного обеспечения и ресурсов;
- *защита по питанию* всего оборудования (ПК, маршрутизаторы и пр.), расположение серверной и коммуникационной техники в отдельно приспособленных помещениях с ограниченным доступом и климат контролем, наличие резервных мощностей для наиболее критичных узлов (например, использование серверов с резервированием);
- *обязательное пользовательское тестирование*, настройка нового оборудования и программного обеспечения в лабораторных условиях перед вводом в эксплуатацию;
- *определение регламентов резервирования* данных, периодическое резервное копирование и архивирование корпоративных данных;
- периодическое *создание образов* системного ПО серверов и рабочих станций для быстрого восстановления систем;
- *физическое резервирование* наиболее критичных серверов, создание кластеров и пр.

3. Работа с внешними поставщиками и подрядчиками, аутсорсинг:

- *определение правил* работы с поставщиками услуг и подрядчиками, *выделение руководителя проекта* со стороны заказчика;
- *завершение* всех проектных работ комплексным пользовательским *тестированием, обучением* пользователей и периодом *опытной эксплуатации*, устранение всех неопределенностей перед внедрением;
- выполнение всех ИТ-работ внутри компании только с представителем ИТ-подразделения;
- наличие альтернативных ресурсов для услуг, используемых в виде аутсорсинга (например, хостинг).

4. Защита от внешних и внутренних воздействий, ограничения прав, криптозащита:

- *описание мероприятий*, направленных на предотвращение утечки информации и несанкционированного доступа;
- *определение правил* доступа и работы сотрудников с информационной системой, в т.ч. ответственности по защите от вирусов;
- *выбор технологий* передачи информации, использование шифрования (при необходимости);

- *выработка процедур контроля* работы информационной системы (протоколирование событий, анализ протоколов, анализ сетевого трафика, анализ работы технических средств);

- *непрерывный мониторинг* – использование аппаратно-программных средств защиты (межсетевые экраны, антивирусные программы) и ручного мониторинга;

- *физическая защита* и защита помещений, техники и бумажной документации от посторонних органов и лиц.

III. ОБЪЕКТЫ ЗАЩИТЫ

Объектами защиты является вся информационно-технологическая инфраструктура компании, а именно, помещения, компьютерное, периферийное, сетевое оборудование и каналы связи, носители информации и программное обеспечение, данные и информация, функционирование документооборота и бизнес-процессов, внутрифирменная конфиденциальная информация, т.е. все элементы бизнеса, нарушение и доступ к которым ведут к ущербу и потерям бизнеса.

Подлежащая защите информация может находиться на бумажных носителях, в электронном виде, передаваться в виде электрических сигналов (телефон, телефакс, телекс), присутствовать в виде акустических и вибросигналов в воздушной среде помещений, записываться и воспроизводиться с помощью технических средств (диктофоны, видеомагнитофоны).

Здесь же **ИБ** конкретизируется **в узком понимании** - как комплекс инструментов по защите программно-технических средств. Она должна обеспечивать выполнение трех основных условий:

1. Программно-технические средства *должны исправно работать* в соответствии с установленной конфигурацией и настройками.

2. На программно-технических средствах должно *выполняться только разрешенное программное обеспечение* – любые другие программы, вирусы, трояны, даунлоадеры, внешние программы не должны попадать и активизироваться в системе.

3. *Доступ* к внутренним ресурсам информационной системы должны иметь *только авторизованные субъекты* согласно своим правам.

IV. ОСНОВНЫЕ КЛАССЫ УГРОЗ

Под **угрозами** ИБ понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

1. *Недоступность информации в результате ее блокирования, сбоя* оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств.

2. *Утрата сведений*, составляющих коммерческую тайну, секреты и иную защищаемую информацию, а также *искажение* (несанкционированная модификация, подделка) такой информации;

3. *Утечка* – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.), а также утечка информации по каналам связи и за счет побочных электромагнитных излучений;

Источники угроз ИБ компании подразделяются на:

- ***внутренние***, вызванные действиями сотрудников, авторизованных пользователей информационной системы – доступ и кража конфиденциальной информации, преднамеренное искажение или уничтожение информации в системе, выполнение манипуляций, приводящих к искажению работы системы или ее сбою,

несоблюдение элементарных правил безопасной работы с почтой, активными элементами на web-страницах, повреждение данных в результате неосторожных действий и т.д.;

- ***внешние***, вызванные внешними воздействиями – сетевые атаки и несанкционированное проникновение в компьютерные сети, вирусы и черви из электронной почты и web-страниц, спам, перехват незашифрованного трафика и т.д.;

- ***естественно-технические и чрезвычайные***, вызванные неправильной эксплуатацией оборудования и неправильным хранением данных, кражей или изъятием компьютеров, бумажных и электронных носителей, форс-мажорными обстоятельствами, выходом из строя и пр.

Весь **перечень** источников угроз может быть следующий:

- стихийные бедствия (пожары, наводнения и т.п.);
- технические аварии (внезапное отключение электропитания, протечки и т.п.);
- несанкционированное получение идентификаторов пользователей и их паролей, паролей доступа к общим ресурсам;
- несанкционированная передача защищаемой информации из внутренней (локальной) сети в глобальную сеть Интернет;
- умышленное или неумышленное разглашение защищаемой информации;
- хищение / изъятие носителей информации или несанкционированное копирование информации;
- хищение / изъятие, физический вывод из строя технических средств;
- посылка в сеть пакетов, нарушающих нормальную работу сети (ложные ARP-запросы и ARP-ответы, перегрузка стеков IP, широковещательные "штормы" и т.д.);
- внедрение программ-троянов, резидентных программ, обеспечивающих получение полного контроля над компьютером; внедрение деструктивных программ – вирусов, сетевых червей и пр.;
- проникновение зловредных программ через Internet (копирование "зараженных" файлов, через апплеты языка Java и объекты ActiveX), электронную почту, гибкие диски, CD-диски;
- получение информации о топологии сети, принципах ее функционирования, характеристической информации сети или участка сети;
- прослушивание сетевого трафика (с целью получения информации о сетевых ресурсах, кешированных паролях, идентификаторах пользователей и пр.) с использованием легальных рабочих станций;
- прослушивание сетевого трафика с использованием нелегальных компьютеров, подключенных к сети физически (локально) или удаленно (Telnet, HTTP);
- внедрение технических и программных средств скрытного съема информации с рабочих станций, средств связи, из помещений компании, в которых обрабатывается защищаемая информация;
- использование специальных методов и технических средств (побочные излучения, наводки по цепям питания, электронные закладки, дистанционное скрытое видео наблюдение или фотографирование, применение подслушивающих устройств, перехват электромагнитных излучений и наводок и т.п.);
- использование для доступа к информации так называемых "люков", "дыр" и "лазеек" и других возможностей обхода механизма разграничения доступа, возникающих вследствие несовершенства общесистемных компонентов программного обеспечения операционных систем, систем управления базами данных и др., неоднозначностями

языков программирования, применяемых в автоматизированных системах обработки данных;

- незаконное подключение специальной регистрирующей аппаратуры к устройствам или линиям связи (перехват модемной и факсимильной связи);
- умышленное изменение используемого программного обеспечения с целью несанкционированного сбора защищаемой информации и т.д.

V. ОПРЕДЕЛЕНИЕ РИСКОВ

Негативные последствия угроз:

- финансовые потери, связанные с утечкой или разглашением защищаемой информации (ущерб, связанный с нарушением конфиденциальности);
- финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации и ресурсов (ущерб, связанный с нарушением целостности, доступности информационных ресурсов и т.д.);
- ущерб от дезорганизации деятельности компании, простоев и потери, связанные с невозможностью выполнения им своих обязательств;
- моральные потери, ущерб репутации компании.

Решение о защите конкретных информационно-технологических ресурсов и степени защиты, финансовые и технические решения принимаются исходя из ценности ресурсов по критериям возможных рисков и вероятности угроз.

VI. МЕРЫ ОБЕСПЕЧЕНИЯ ИБ

Общими мерами по обеспечению ИБ компании являются:

- административно-правовые, организационные и режимные;
- технические, основанные на использовании аппаратно-программных и специальных средств.

Обобщенный перечень ***административно-правовых и организационных мер:***

1. Определение правового статуса всех субъектов отношений в информационной среде, установление их ответственности перед компанией через соблюдение нормативных актов, регламентов и политик в сфере ИБ.
2. Включение в должностные инструкции сотрудников обязанностей и ответственности по ИБ. Разработка правил эксплуатации технических и программных средств (регламентов, порядков) и правил реагирования при нарушении режима безопасности (подозрений на нарушение).
3. Обучение всех сотрудников вопросам обеспечения ИБ компании. Подготовка и повышение квалификации ИТ-сотрудников в области ИБ. Регламентирование работы сотрудников охраны.
4. Аттестация информационных объектов на защищенность при необходимости.
5. Обеспечение преемственности при разработке технологических и программных решений. Оперативное реагирование (внедрение) на появление новых разработок в области информационных технологий.
6. Обеспечение принципа разграничения доступа: информация должна быть доступна только тем, кому она предназначена и разрешена. Предоставление сотрудникам минимально достаточных прав по доступу к информации, необходимых для выполнения ими своих функциональных обязанностей.
7. Создание эффективной системы контроля за выполнением требований локальных нормативных актов ИБ. Пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации.

8. Разработка перечня возможных нарушений ИБ и локальных нормативных актов. Совершенствование нормативно-правовой базы по работе с конфиденциальной информацией и сведениями внутри компании и со сторонними организациями. Разработка *Руководства по ИБ* – оперативного документа ежедневного использования, содержащего детальные рабочие инструкции.

Обобщенный перечень ***режимных мер:***

1. Определение пропускного и внутриобъектового режима в компании, разграничение доступа и контроль за доступом в выделенные помещения; инструктаж сотрудников охраны;
2. Определение перечня критичной внутренней документации компании, мест и сроков ее хранения, порядок доступа и уничтожения.
3. Определение мероприятий и действий при чрезвычайных обстоятельствах для всех подразделений и служб.

Обобщенный перечень ***технических мер:***

1. Обеспечение безотказной работы аппаратных средств, резервирование, спецпомещения.
2. Использование лицензионного программного обеспечения; заказного программного обеспечения, прошедшего этап тестирования и опытной эксплуатации.
3. Использование сертифицированных средств защиты информации для обработки, хранения и передачи конфиденциальной информации, при необходимости использование защищенных соединений с шифрованием, в частности, для удаленных соединений.
4. Проведение комплексной антивирусной защиты.
5. Внедрение в сеть современной системы обнаружения вторжений, мониторинг несанкционированного подключения к информационным ресурсам.
6. Проведение эффективной парольной защиты. Использование единственной системы авторизации пользователей и разграничения прав доступа к ресурсам сети на базе доменной поддержки операционной системы.
7. Проведение контроля состояния программного и информационного обеспечения компьютеров (состава и целостности программного обеспечения, корректности настроек и т.д.) и маршрутизаторов (маршрутных таблиц, фильтров, паролей).
8. Обеспечение резервного копирования.
9. Проведение мониторинга за деятельностью пользователей (вход-выход в систему, доступ к сетевым ресурсам и пр.), проведение контроля трафика сети на отдельных ее сегментах.
10. Использование внутренних IP-адресов из диапазона, специально выделенного для построения частных сетей. Создание «демилитаризованной зоны» на стыке локальной сети компании и внешней сети.
11. Выделение отдельной изолированной подсети для экспериментов по освоению новых технологий и тестированию программного обеспечения, либо использования VMware сред.
12. Определение действий по резервному копированию и защите информации при чрезвычайных обстоятельствах.

Задача обеспечения ИБ должна решаться **системно**. Это означает, что различные средства защиты (аппаратные, программные, физические, организационные и т. д.)

должны применяться одновременно, на всех уровнях информационного взаимодействия и под централизованным управлением. При этом компоненты системы должны "знать" о существовании друг друга, взаимодействовать и обеспечивать защиту как от внешних, так и от внутренних угроз.

Арсенал технических методов обеспечения ИБ широк и подбирается после анализа всех рисков:

Уровни безопасности	*Применяемые меры безопасности*
Периметр	Межсетевой экран, антивирус для шлюзов, VPN, анализаторы контента, IPS (Intrusion Prevention Systems — системы предотвращения вторжений), PKI-решения (Public Key Infrastructure — доверительные отношения с помощью цифровых сертификатов, подписываемых центром сертификации)
Сеть	IDS (Intrusion Detection Systems — системы обнаружения вторжений), межсетевое экранирование, сканнеры оценки уязвимости (Vulnerability-Assessment - VA), аутентификация, управление доступом, управление политиками безопасности, средства контроля содержимого электронной почты, средства контентной фильтрации, защита от утечки по техническим каналам, системы мониторинга событий, защита телефонных систем
Хост	Host IDS, системные сканеры, анализаторы политик безопасности, антивирусы, управление доступом, аутентификация
Приложения	Контроль ввода данных, Host IDS, анализаторы политик безопасности, контроль доступа, аутентификация
Данные	Криптографическая защита (шифрование, подпись), управление доступом, аутентификация

6. Устный зачет по Теме 3

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Для чего используется и каковы особенности ЭП – электронной цифровой подписи?
2. Как предпочтительнее передавать открытые ключи PGP своим корреспондентам?
3. Что влияет на криптостойкость ЭП?
4. Какой ключ используется при шифровании сообщения?
5. Какой ключ используется при создании цифровой подписи?
6. Какие системы создания ЭП и шифрования используются в России?
7. Как отправлять файлы на защищенное хранение при помощи программы PGP?
8. С помощью каких программ можно обеспечить защищенное хранение файлов?
9. Существует ли вероятность потери (удаления) защищенных файлов?

Эталоны ответов: приведены в Учебном пособие по дисциплине «Правовое обеспечение информационной безопасности».

7. Практическая работа № 10. Проведение аудита состояния информационной безопасности предприятия

Инструкция для обучающихся
Внимательно прочитайте задание. Разработайте проект отчета аудита состояния информационной безопасности предприятия.

Время выполнения задания – 60 минут.

Задание

1. Используя план по проведению аудита, разработайте проект отчета аудита состояния информационной безопасности предприятия
2. При разработке проекта отредактируйте текст положения с учетом особенностей Вашей организации.
3. Оформление проекта положения должно соответствовать требованиям ГОСТ 7.0.97-2016.

Текст ГОСТа можно прочитать здесь:

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Пример плана по проведению аудита

1. Цель проекта
2. Подход к выполнению работ
3. Резюме для руководства о результатах проведенного аудита
4. Результаты анализа технической защищенности внешнего периметра
4.1 Описание используемых средств
4.2 Описание выявленных недостатков/уязвимостей в отношении внешнего периметра
5. Результаты анализа защищенности внутреннего периметра
5.1. Область проведения
5.2. Описание выявленных недостатков/уязвимостей в отношении внутреннего периметра
5.3. Описание выявленных недостатков/уязвимостей в отношении DMZ
6. Рекомендуемые шаги

Вставьте ниже разработанный проект

Эталон ответа:
1. Цель аудита
Целью проекта является проведение независимого технического аудита информационной безопасности. Следующие задачи были обозначены как ключевые в отношении проведения комплексного аудита ИБ:

- получение оценки текущего уровня защищенности сетевой инфраструктуры;
- разработка рекомендаций по повышению уровня защищенности и устранению выявленных уязвимостей.

2. Подход к выполнению работ
В рамках проекта моделировались действия следующих категорий нарушителей:

- **Внешний нарушитель**: нарушитель, не обладающий знаниями об ИТ-инфраструктуре Компании, не имеющий возможности доступа в офис и не имеющий возможности подключения к локальной сети Компании.
- **Внутренний нарушитель**: нарушитель, имеющий возможность доступа в офис и физического подключения к ЛВС Компании.

В рамках оценки степени выполнения основных положений рассматривались следующие критерии:

- Текущий уровень ИБ:
  - распределение ролей;
  - управление доступом и регистрация;
  - антивирусная защита; - использование Интернет.
- Менеджмент ИБ:
  - функционирование службы ИБ;
  - оценка и обработка рисков ИБ;
  - документирование деятельности в области ИБ;
  - реагирование на инциденты безопасности;

3. Резюме для руководства о результатах проведенного аудита

<table>
<tr><th>Внешнее тестирование</th><th>Внутреннее тестирование</th><th>Оценка организационного обеспечения безопасности</th></tr>
<tr><td rowspan="2">В рамках работ по тестированию защищенности внешнего периметра была проведена идентификация уязвимостей в отношении внешних адресов Компании.
• В результате идентификации уязвимостей было обнаружено наличие 1 критичной уязвимости, 2 уязвимостей среднего уровня критичности, 1 уязвимости низкого уровня критичности.
• Обнаруженные уязвимости связаны с отсутствием своевременного обновления используемого программного обеспечения и некорректной настройкой используемого программного обеспечения.
• Рекомендации по исправлению выявленных уязвимостей приведены при описании конкретных</td><td colspan="2">В рамках работ по тестированию Для оценки организационного обеспечения защищенности внутреннего периметра безопасности информации Исполнителем была проведена идентификация применялся подход, описанный в СТО БР уязвимостей в отношении узлов, ИББС образующих локальную инфраструктуру • В рамках оценки степени выполнения Банка и узлов демилитаризованной зоны основных положений СТ (DMZ). оценка текущего уровня ИБ и • Критичные уязвимости были обнаружены менеджмента ИБ. как автоматическими средствами • Уровень ИБ и Менеджмент И</td></tr>
<tr><td>сканирования, так и в ходе экспертного анализа.
• Обнаруженные уязвимости связаны с отсутствием в Компании политики и правил управления паролями, учетными записями, отсутствием своевременного обновления ПО, некорректной настройкой используемого ПО и сетевого оборудования.
• Рекомендации по исправлению выявленных</td><td>Компания не соответствуют требуемому согласно СТО БР ИББС уровню ни по одному из групповых показателей, по которым осуществлялась оценка. Менеджмент ИБ в настоящий момент находится в критическом состоянии.</td></tr>
</table>

уязвимостей.	уязвимостей приведены в разделе по описанию результатов внутреннего тестирования.	

По результатам проведенных работ можно сделать следующие выводы:

- Текущее управление информационной безопасностью Компании имеет проблемы системного характера: выявленные технические уязвимости имеют общие причины возникновения и присутствуют во всех рассмотренных системах
- В Компании отсутствуют базовые элементы управления информационной безопасности: стандарты по ИБ, политики и процедуры, правила, система контроля соблюдения требований по ИБ
- Организационная и техническая системы ИБ требуют существенного улучшения
- Как результат, текущий уровень защиты информационных систем находится ниже общепринятого базового уровня
- Необходимо принять меры организационного и технического характера

4. Результаты анализа технической защищенности внешнего периметра

4.1 Описание используемых средств

Настоящий раздел содержит описание результатов проведения экспертного и инструментального анализа внешней ИТ-инфраструктуры с участием профильных специалистов.

Инструментальное исследование внешнего сетевого периметра проводилось с использованием следующих средств по анализу защищенности:

MaxPatrol

MaxPatrol – программное средство контроля защищенности сетевой инфраструктуры. Позволяет получать объективную оценку защищенности информационных систем. Существует возможность использования следующих профилей для проверки сети:

- тестирование на проникновение (Pentest);
- системная проверка (Audit);
- контроль соответствия стандартам (Compliance).

Программное средство сертифицировано по требования безопасности информации, сертификат соответствия №2305 действителен до 24 марта 2014 года.

Cain&Abel

Утилита для восстановления паролей, прослушивания сетевого трафика, декодирования защищенных паролей, восстановления ключей беспроводных сетей и анализа маршрутизации протоколов. Применялась для осуществления проверки уязвимости сетевой инфраструктуры к атаке ARP-poisoning.

Intercepter

Многофункциональный снифер паролей и переписки. Осуществляет перехват паролей\хешей следующих протоколов:

- ICQ\IRC\AIM\FTP\IMAP\POP3\SMTP\LDAP\BNC\SOCKS\HTTP
- \WWW\NNTP\CVS\TELNET\MRA\DC++\VNC\MYSQL\ORACLE

Осуществляет перехват переписки следующих протокол ICQ\AIM\JABBER\YAHOO\MSN\IRC\MRA
Проводит MiTM атаки: ARP\DHCP\DNS over ICMP\SSL\SSLSTRIP
Nmap

В область проведения анализа технической защищенности внешнего периметра по согласованию с представителями Заказчика были включены следующие внешние ресурсы Заказчика:

Основная внешняя подсеть 195.xx.yyy.0/24

- 213.xx.yyy.8/29
- 213.xx.yyy.32/27
- 213.xx.yyy.0/27

В отношении вышеперечисленных хостов специалистами были проведены следующие процедуры:

- Сбор информации о запущенных службах;
- Обработка и интерпретация собранной информации;
- Поиск и анализ уязвимостей;
- Описание выявленных уязвимостей.

4.2 Описание выявленных недостатков/уязвимостей в отношении внешнего периметра

195.xx.yyy.3 (ns-m.company.ru)
143/TCP - IMAP 110/TCP - POP3

Небезопасный метод аутентификации:

Удаленный сервер допускает использование незашифрованных учетных данных, передаваемых по незащищенному протоколу. Это позволяет злоумышленникам, при помощи прослушивания, получить информацию об имени и пароле пользователя.

POP3	IMAP
Методы аутентификации	Методы аутентификации
LOGIN	IMAP LOGIN
PLAIN	LOGIN
USER/PASS	PLAIN

Решение:

Настройка службы на использование пониженного уровня безопасности аутентификации только для шифрованных соединений.

CVSS	
Базовая	2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS	
оценка	
AV:N	данная уязвимость может эксплуатироваться удаленно
AC:H	для эксплуатации уязвимости нужны особые условия, или уязвимая конфигурация редко встречается на практике
Au:N	для эксплуатации уязвимости проходить аутентификацию не требуется

C:P	эксплуатация уязвимости влечет существенное разглашение
I:N	эксплуатация уязвимости не затрагивает целостность системы
A:N	эксплуатация уязвимости не влияет на доступность системы

Ссылки:

- http://tools.ietf.org/html/rfc4422
- http://tools.ietf.org/html/rfc4954

195.xx.yyy.4 (ns1.company.ru)

53/UDP - BIND Server (Версия: 9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6.3)

Использование памяти после освобождения

Уязвимость позволяет атакующему вызвать отказ в обслуживании. Уязвимость в ISC BIND (BIND-форум) позволяет злоумышленникам, действующим удаленно, вызвать отказ в обслуживании (аварийное завершение работы named-демона), что приводит к «разыменованию ранее освобожденной выборки контекста».

Решение:

Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Необходимую информацию можно получить по адресу: http://www.securityfocus.com/bid/22229/solution

CVSS	
Базовая оценка	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
Временная оценка	3.2 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:U/RL:OF/RC:C)
AV:N	данная уязвимость может эксплуатироваться удаленно
AC:H	для эксплуатации уязвимости не требуются особые условия
Au:N	для эксплуатации уязвимости проходить аутентификацию не требуется
C:N	эксплуатация уязвимости не затрагивает конфиденциальные данные
CVSS	
	системы
I:N	эксплуатация уязвимости не затрагивает целостность системы
A:C	при успешной эксплуатации злоумышленник может сделать систему полностью недоступной

Ссылки:

- FULLDISC (20070125 BIND remote exploit (low severity) [Fwd: Internet Systems Consortium Security Advisory.]): http://lists.grok.org.uk/pipermail/full-disclosure/2007January/052018.html
- MLIST ([bind-announce] 20070125 Internet Systems Consortium Security Advisory.): http://marc.theaimsgroup.com/?l=bind-announce&m=116968519321296&w=2
- http://www.isc.org/index.pl?/sw/bind/view/?release=9.2.8

- http://www.isc.org/index.pl?/sw/bind/view/?release=9.3.4
- FRSIRT (ADV-2007-0349): http://www.frsirt.com/english/advisories/2007/0349
- SECUNIA (23904): http://secunia.com/advisories/23904
- BUGTRAQ (20070125 BIND remote exploit (low severity) [Fwd: Internet Systems Consortium Security Advisory http://www.securityfocus.com/archive/1/archive/1/458066/100/0/threaded

195.xx.yyy.6 (ibank2.company.ru)
195.xx.yyy.8 (plastic.company.ru)
443/TCP - HTTP SSL (ibank2.company.ru)
8080/TCP – HTTP (plastic.company.ru)

Возможна атака Anti DNS Pinning

Сервер уязвим для обхода ограничений политики безопасности Same Origin Policy с помощью атаки Anti DNS Pinning (DNS rebinding).

Описание:

Атака Anti DNS Pinning (DNS rebinding) позволяет злоумышленнику манипулировать соответствием между IP-адресом и DNS-именем узла (FQDN) с целью запуска активного содержимого в контексте безопасности уязвимого сайта. Используя эту технику, злоумышленник может использовать браузер жертвы для получения доступа к защищенным сайтам (например, находящимся за межсетевыми экранами или требующим аутентификации). В отличие от атаки типа «Подделка межсайтового запроса» (Cross-Site Request Forgery, CSRF), атака Anti DNS Pinning направлена на получение данных (нарушение конфиденциальности) а не на выполнение каких-либо действий с приложением (нарушение целостности). Однако совместно с CSRF атака Anti DNS Pinning может использоваться для полнофункционального доступа к веб-приложению через браузер пользователя.

Проблема настройки сервера состоит в том, что он не осуществляет достаточную проверку поля Host в HTTP-запросе. При поступлении запросов с произвольным адресом в поле Host сервер должен возвращать ошибку.

Решение:

Удаление стандартных виртуальных сайтов, отвечающих на HTTP-запросы с произвольным значением заголовка HOST. В IIS для этого необходимо установить непустое значение «Host header value» для всех веб-сайтов. В Apache необходимо установить непустое значение директивы ServerName для всех виртуальных сайтов (даже если сайт на сервере один, он должен быть оформлен в виде Virtual Host) и проверить что сайт по умолчанию ни указывает на другие сайты, а возвращает ошибку.

CVSS	
Базовая оценка	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
AV:N	данная уязвимость может эксплуатироваться удаленно
AC:H	для эксплуатации уязвимости нужны особые условия, или уязвимая конфигурация редко встречается на практике
Au:N	для эксплуатации уязвимости проходить аутентификацию не требуется
C:C	эксплуатация уязвимости влечет полное разглашение конфиденциальных данных
I:N	эксплуатация уязвимости не затрагивает целостность системы

A:N	эксплуатация уязвимости не влияет на доступность системы

Ссылки:

- https://www.blackhat.com/presentations/bh-usa-07/Byrne/Presentation/bh-usa-07-byrne.pdf
- http://www.servletsuite.com/servlets/hostflt.htm
- http://ha.ckers.org/blog/20060908/dns-pinning-just-got-worse/

5. Результаты анализа защищенности внутреннего периметра

5.1 Область проведения

В область проведения анализа технической защищенности внешнего периметра по согласованию с представителями Заказчика были включены следующие внутренние ресурсы Заказчика:

- 192.168.10.0/24
- 192.168.9.0/24
- 192.168.7.0/24

Ресурсы демилитаризованной зоны (DMZ):

- 172.35.1.0/24
- 172.25.1.0/24

В отношении вышеперечисленных хостов специалистами были проведены следующие процедуры:

- Сбор информации о запущенных службах;
- Обработка и интерпретация собранной информации;
- Поиск и анализ уязвимостей;
- Описание выявленных уязвимостей.

5.2 Описание выявленных недостатков/уязвимостей в отношении внутреннего периметра

Использование легкоподбираемых реквизитов доступа или реквизитов доступа «по умолчанию»:

Получен доступ к NAS 192.168.10.2 с логином root без пароля, причем доступ возможен как через WEB-интерфейс, так и по ssh.

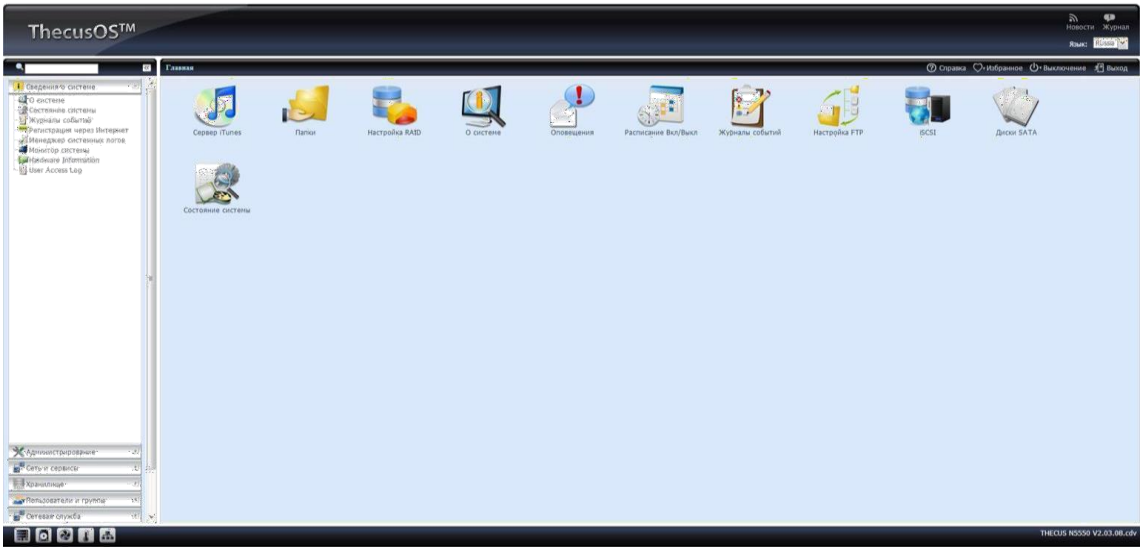


Рисунок 1. Доступ к 192.168.10.2

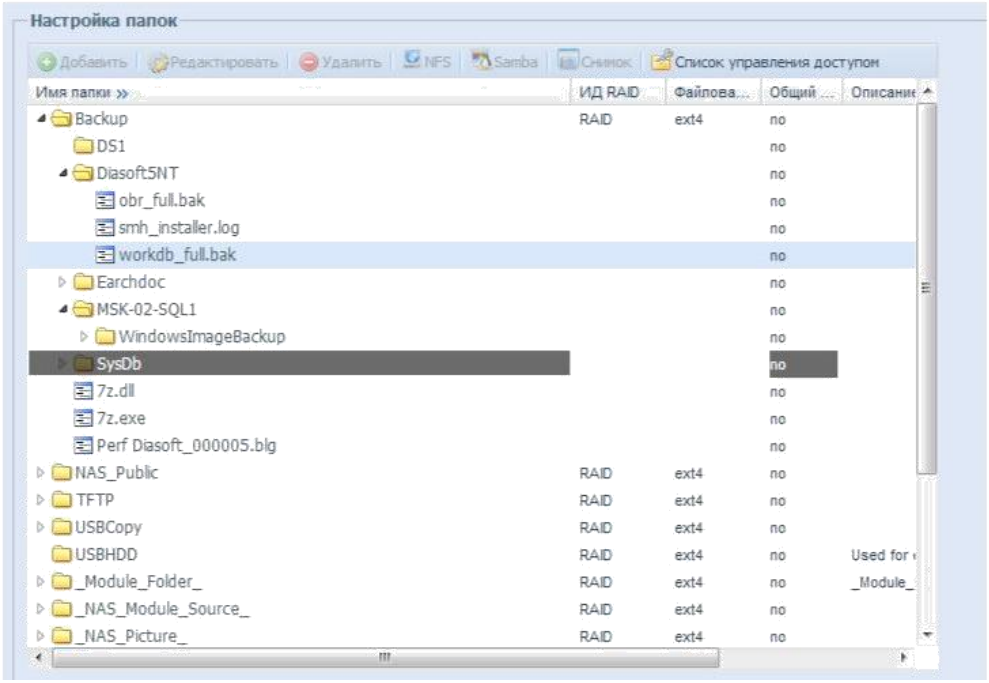


Рисунок 2. Доступ к 192.168.10.2

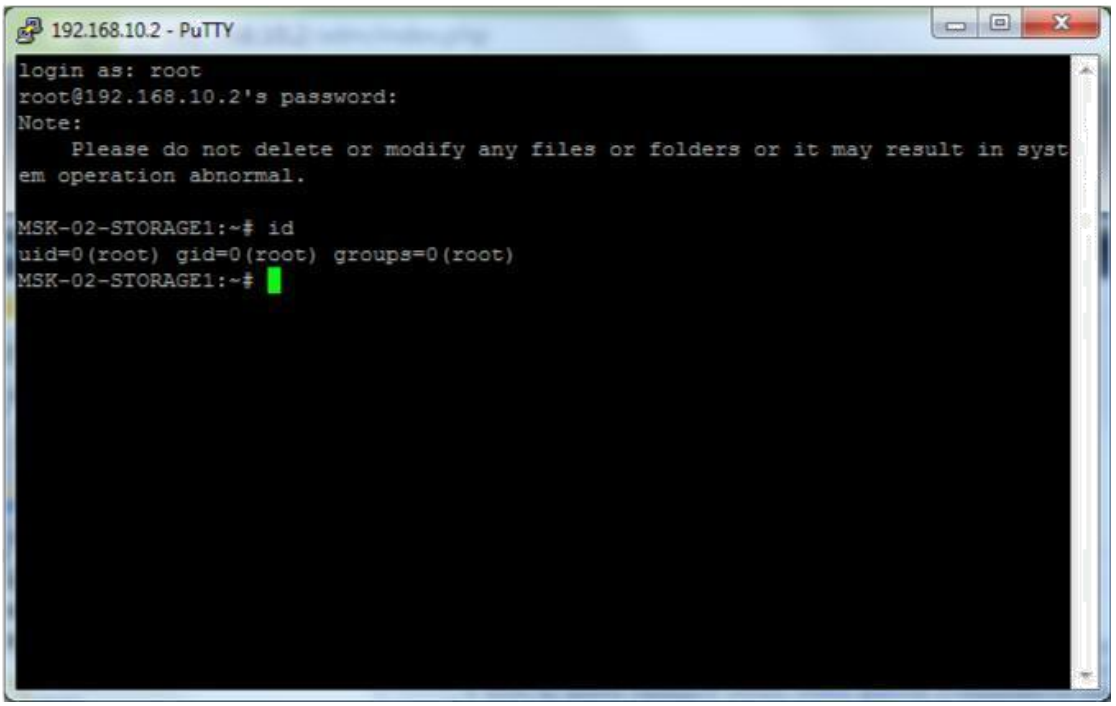


Рисунок 3. Доступ к 192.168.10.2 по ssh с логином root без использования пароля

В результате получены следующие данные пользователей

NAS:

root:1xYbh5DFV$YeLEggrjD/a2KfvUurY7Q0:0:0:root:/root:/b
in/sh rpcuser:*:29:492:RPC Service User:/var/lib/nfs:

- rpc:*:32:32:Rpcbind Daemon:/var/lib/rpcbind:
- sshd:*:33:33:sshd:/:
- ftp:*:50:50:ftp:/raid/data/ftproot:/dev/null
- admin:1yn9JM4EL$9MqDN2QOQ3PVwF7.dJmeU/:97:97:admin:/dev/null:/dev/null
  nobody:*:99:99:nobody:/:

- adminstorage:$1$6N.oztVZ$frocyTufL9zz7iU5FJ8QJ1:1000:100:adminstorage:/dev/null:/de v/null
- backuper:1z7H2xe5J$4J9KAOaUv.i6.lSDky.F31:1001:100:backuper:/dev/null:/dev/null

На СХД хранятся чувствительные данные Компании, в том числе были обнаружены следующие файлы данных:

- backup.db
- passdb.tdb
- ad_account.db
- smb.db
- USERS01.DBF
- secrets.tdb

Получен доступ к серверу 192.168.10.3:

Реквизиты доступа:
Login: User
Password: (empty)

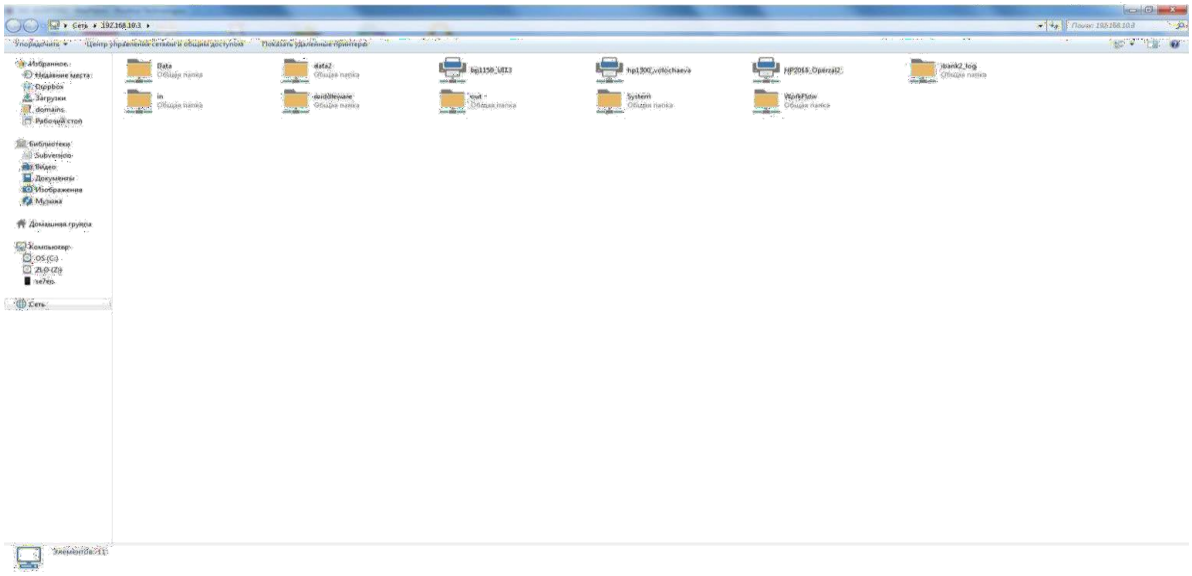


Рисунок 4. Получен доступ к серверу 192.168.10.3

Сервер 192.168.10.13 отдает пароль с помощью специального запроса:

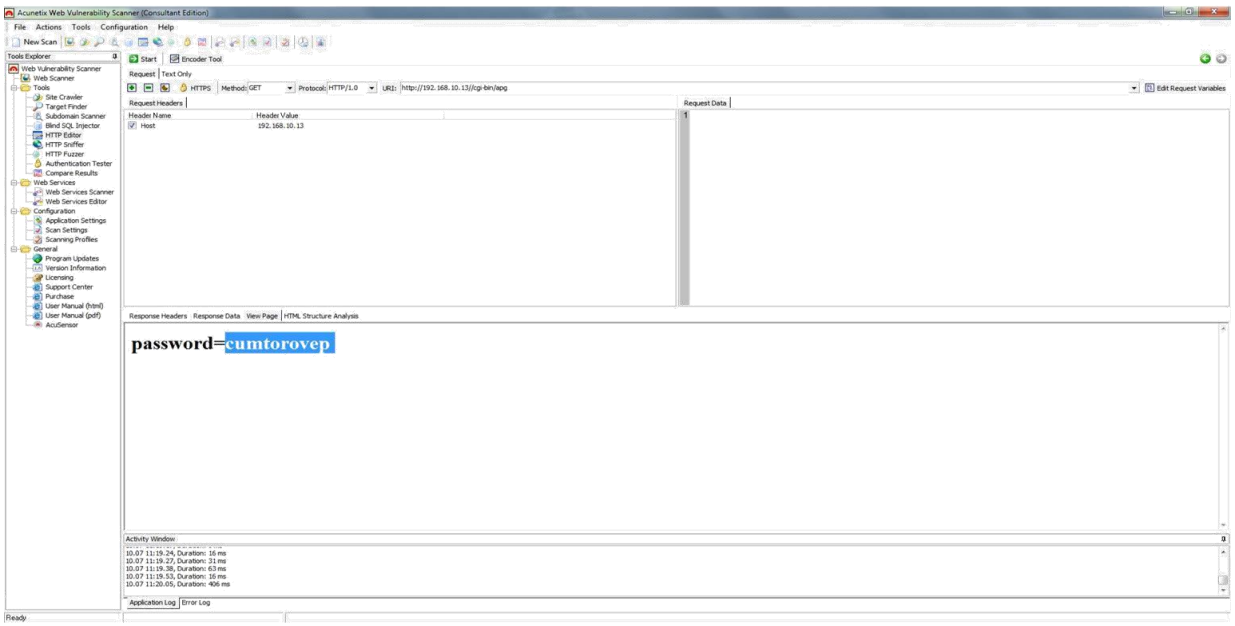


Рисунок 5. Пароль в открытом виде на 192.168.10.13

В результате доступа к серверу 192.168.10.13 удалось получить содержимое файла hosts и дополнительную информацию о сетевой инфраструктуре:

192.168.10.1 dfl-b16-1
192.168.10.2 terminal-b16
192.168.10.3 abs-b16
192.168.10.4 sadko-b16
192.168.10.5 term4
192.168.10.6 msr30-b16f2-vlan10
192.168.10.7 kerio-b16 ns-e
192.168.10.8 term5
192.168.10.11 nsrv-b16
192.168.10.13 noc
192.168.10.14 term2
192.168.10.15 cronos-b16
#192.168.10.16 ds5
192.168.10.17 b21-b16
192.168.10.18 msr30-b16f3-vlan10
192.168.10.19 nsrv2-b16
192.168.10.22 msk-02-dc1
192.168.10.50 ds1
192.168.10.51 ds2
192.168.10.52 ds4
192.168.10.53 msk-02-sql2
192.168.10.55 logic
192.168.10.59 msk-02-sql1
192.168.10.62 ds5
#192.168.7.240 hp2610-b16f3-phone1
#192.168.7.241 hp2520-b16f2
#192.168.7.242 hp2610-b16f2-phone2
192.168.7.250 pbxnsip nsip sip
/B16
NOVOSIBIRSK
192.168.1.254 srx-nsk
192.168.1.251 pbx-nsk
/NOVOSIBIRSK
LENIN
192.168.5.7 kerio-lp63 kerio-lenin gw-lenin
192.168.5.8 ns0-lp63
192.168.5.254 srx-lp63
/LENIN

#192.168.10.105 esxi-voip3
192.168.10.240 a5500-b16f2-vlan10
192.168.10.253 msr30-b16-vrrp-vlan10
192.168.10.254 dfl-b16
##
192.168.9.12 msk-02-dc2
192.168.9.69 msk-02-b22
####Guest wifi####
172.16.2.254 gwifi
##########16 NETWORK VTS#################
192.168.16.1 msk-02-vts1
192.168.16.2 msk-02-vts2
192.168.16.3 msk-02-vts3
192.168.16.4 msk-02-vts4
192.168.16.5 msk-02-vts5
192.168.16.6 msk-02-vts6
192.168.16.7 msk-02-vts7
192.168.16.8 msk-02-vts8
192.168.16.9 msk-02-vts9
192.168.33.254 srx-znamenka
/ZNAMENKA
obrdop8 aka varshavka33
192.168.34.254 srx-do8 dfl-do8
192.168.34.253 hp-do8
/obrdop8 aka varshavka33
obrdop8 aka do8 NEW
192.168.35.254 srx-do8-new
/obrdop8 aka do8 NEW
GILYAROVSKOGO
192.168.39.254 srx-gilyar
/GILYAROVSKOGO
obrdop6
192.168.40.252 apc-do6
192.168.40.254 srx-do6 dfl-do6
/obrdop6

192.168.10.1 dfl-b16-1
192.168.10.2 terminal-b16
192.168.10.3 abs-b16
192.168.10.4 sadko-b16
192.168.10.5 term4
192.168.10.6 msr30-b16f2-vlan10
192.168.10.7 kerio-b16 ns-e
192.168.10.8 term5
192.168.10.11 nsrv-b16
192.168.10.13 noc
192.168.10.14 term2
192.168.10.15 cronos-b16
#192.168.10.16 ds5
192.168.10.17 b21-b16
192.168.10.18 msr30-b16f3-vlan10
192.168.10.19 nsrv2-b16
192.168.10.22 msk-02-dc1
192.168.10.50 ds1
192.168.10.51 ds2
192.168.10.52 ds4
192.168.10.53 msk-02-sql2
192.168.10.55 logic
192.168.10.59 msk-02-sql1
192.168.10.62 ds5
192.168.10.242 bac1 bac1.company.local
SFT
192.168.14.254 srx-sft
PODOLSK
192.168.21.254 srx-podolsk dfl-podolsk
192.168.21.250 cctv-podolsk
/PODOLSK
NET28
192.168.28.254 dfl-net28
/NET28
NSK-STUD
192.168.31.254 srx-nsk-stud
/NSK-STUD

msk-02-

На сервере были обнаружены файлы, содержащие конфигурацию сетевых устройств: DFL, H3C, HP, Juniper. Доступ злоумышленника к подобным файлам может повлечь за собой раскрытие чувствительной информации об особенностях сетевой инфраструктуры, в том числе об используемых маршрутах, протоколах.

Файлы конфигурации содержат пароли администраторов устройств в зашифрованном виде. Отдельные пароли хранятся с помощью небезопасных алгоритмов шифрования и, в связи с этим, специалистам удалось их расшифровать и получить доступ к критичным узлам сети (устройства Juniper).

Рекомендации: не хранить пароли администраторов устройств в формате Juniper 9 Password. Не хранить файлы конфигурации на общедоступном для пользователей локальной сети сервере.

Получен доступ к 192.168.10.50 (ds1) с помощью следующих реквизитов доступа:
Login: test
Password: 123456

Удалось подключиться к базе MS SQL (192.168.10.57) с использованием следующих реквизитов доступа:
Login: test
Password: test

Рисунок 6. Подключение к базе данных MS SQL

Получен доступ к системе резервного копирования (192.168.10.242, bac1 msk-02bac1.company.local) с помощью следующих реквизитов доступа:
Login: root
Password: password

Панель администрирования принтеров в открытом доступе.

Любой пользователь локальной сети банка может получить доступ к панели администрирования сетевого принтера просто обратившись к нему по адресу его размещения, например 192.168.9.3:80

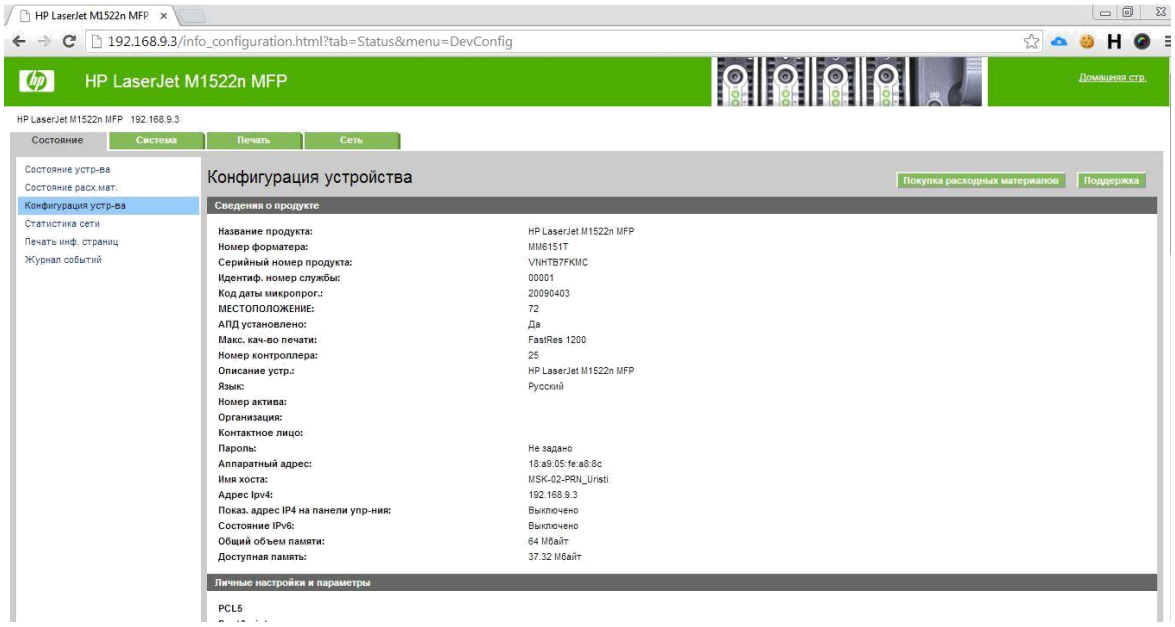


Рисунок 7. Панель управления принтерами

Общие рекомендации:

- Необходимо сменить все подобранные в ходе аудита реквизиты доступа;
- Не использовать пароли по умолчанию для доступа к NAS, серверам, приложениям и сетевым устройствам;
- Не использовать одинаковые пароли для доступа к разнородным устройствам; Для генерации паролей использовать специализированное программное обеспечение (keepass, etc), которое позволяет генерировать пароли заданной сложности.
- Запретить доступ к панели управления принтером без пароля.

ARP-poisoning

Анализ безопасности протокола ARP показывает, что, перехватив на атакующем хосте внутри данного сегмента сети широковещательный ARP-запрос, можно послать ложный ARPответ, в котором объявить себя искомым хостом (например, маршрутизатором), и в дальнейшем активно контролировать сетевой трафик дезинформированного хоста, воздействуя на него по схеме «ложный объект ЛВС».

Атака обычно начинается с прослушивания канала связи и заканчивается тем, что аналитик пытается подменить перехваченное сообщение, извлечь из него полезную информацию, перенаправить его на какой-нибудь внешний ресурс.

Применяя данный вид атаки, злоумышленник может получить доступ к учетной записи пользователя.

В Компании используются текстовые прикладные протоколы передачи данных без наличия средств шифрования, что делает возможным перехват парольной информации в отношении используемых WEB-сервисов для корпоративных приложений, сервисов электронной почты.

Существует возможность перехвата LM&NTLM, NTLMv2 хешей, что делает доступным работу из-под сторонних учетных записей пользователей домена. В результате чего возможен доступ злоумышленника к почте легитимных пользователей, и к любой иной информации, передаваемой в локальной сети.

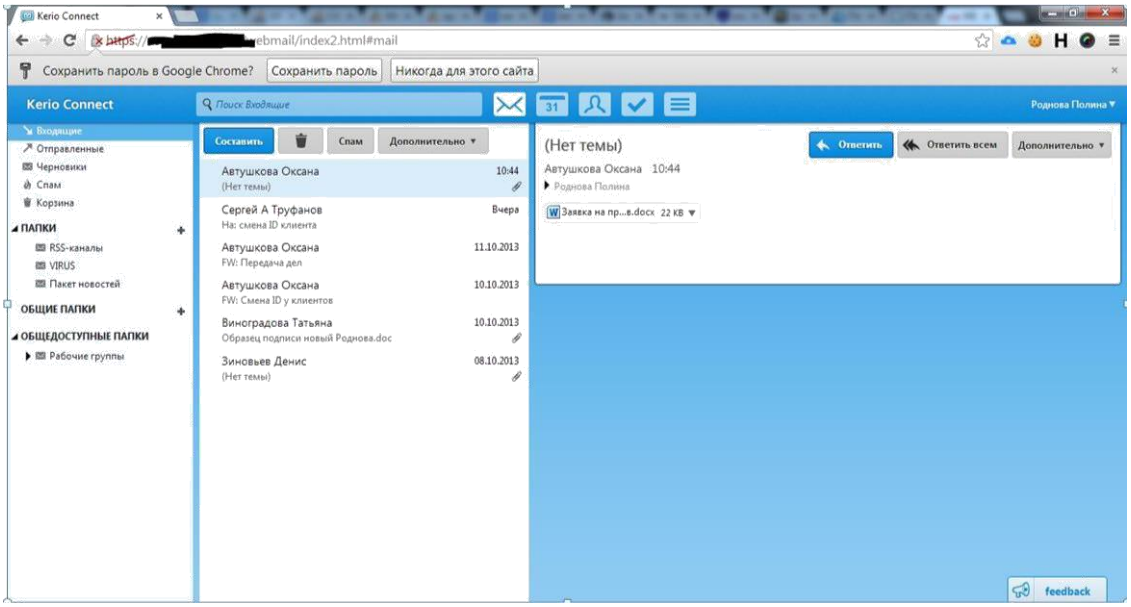


Рисунок 8. Доступ к учетной записи Автушковой Оксаны

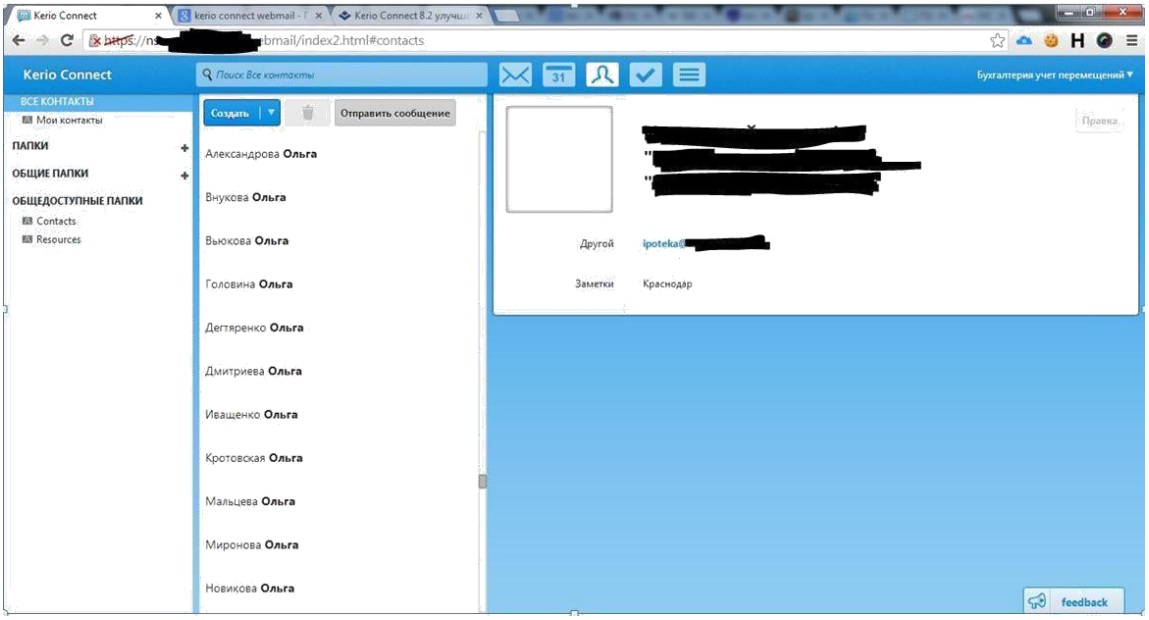


Рисунок 9. Доступ к администрированию почты, создание учетных записей

Доступ к системе nagios (перехвачены логин и пароль: nagiosadmin-qazsedcft):

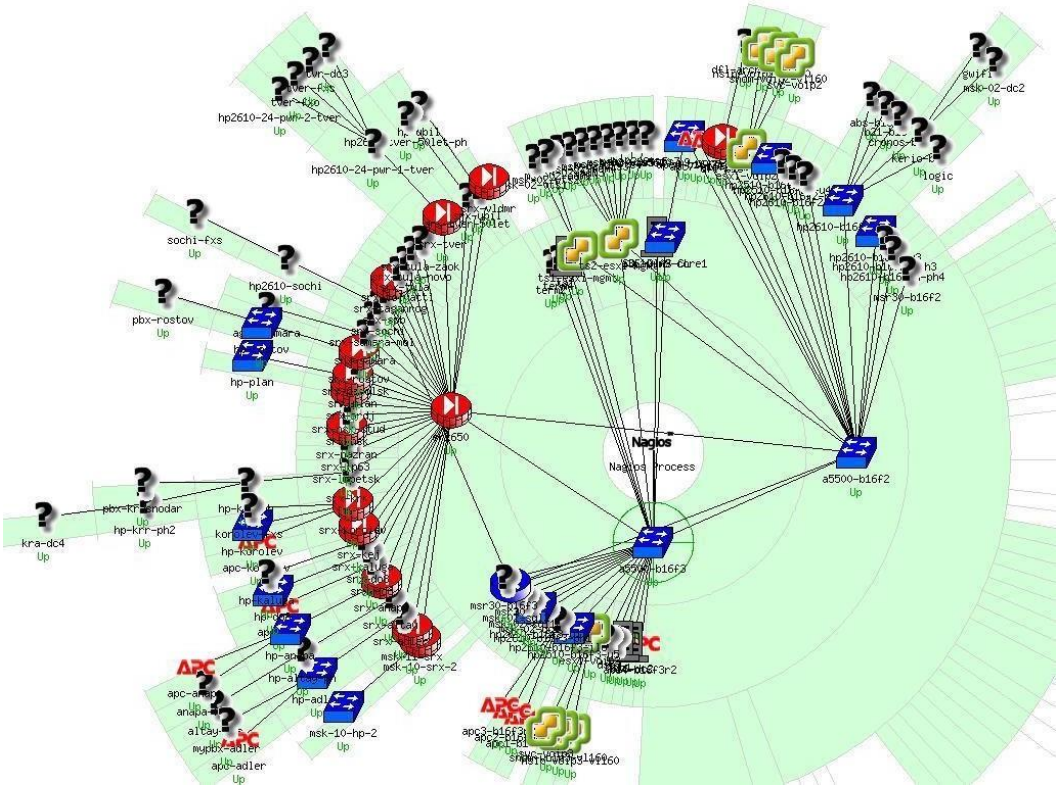


Рисунок 10. Дополнительные данные об особенностях локальной сети

Рекомендации:

Использовать статические записи в таблице ARP

5.3 Описание выявленных недостатков/уязвимостей в отношении DMZ

172.35.1.2 (IBANK2_JAVA)

3389/TCP - Microsoft RDP

Подмена данных в сертификате

Уязвимость позволяет атакующему получить доступ к защищенному трафику. В цепочке сертификатов найден сертификат, который содержит символ \x00 в поле CommonName.

Сертификаты, содержащие символ \x00 в поле CommonName, позволяют злоумышленникам эксплуатировать уязвимость в механизме проверки корректности сертификата, который применяется в различных браузерах, а также других продуктах, использующих SSL. В случае успешной эксплуатации злоумышленник может провести атаку типа "человек посередине" и получить доступ к защищенному трафику.

Решение:

Установите корректный сертификат для данной службы.

CVSS	
Базовая оценка	8.3 (AV:A/AC:L/Au:N/C:C/I:C/A:C)
AV:A	для успешной эксплуатации уязвимости злоумышленник должен иметь доступ к соседней сети
AC:L	для эксплуатации уязвимости не требуются особые условия
Au:N	для эксплуатации уязвимости проходить аутентификацию не требуется

C:C	эксплуатация уязвимости влечет полное разглашение конфиденциальных данных
I:C	эксплуатация уязвимости влечет полное нарушение целостности системы
A:C	при успешной эксплуатации злоумышленник может сделать систему полностью недоступной

Ссылки:

- http://seclists.org/fulldisclosure/2009/Oct/87
- http://www.thughtcrime.org/papers/null-prefix-attacks.pdf

445/TCP - Microsoft DS

Не требуется подписывание SMB

Узел не требует подписывания SMB. Возможно проведение атаки "человек посередине" на SMB-сервер. В настройках SMB-сервера доступны три опции, касающиеся подписывания SMB:

- подписывание SMB включено и обязательно для всех клиентов; подписывание SMB включено, но не обязательно для всех клиентов; подписывание SMB отключено.

Безопасность данных обеспечивает только первый вариант с включенным и обязательным для всех клиентов подписыванием SMB. На данном узле выбран небезопасный вариант настроек.

Решение:

Включить подписывание SMB в настройках сервера.

CVSS	
Базовая оценка	5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
AV:N	данная уязвимость может эксплуатироваться удаленно
CVSS	
AC:L	для эксплуатации уязвимости не требуются особые условия
Au:N	для эксплуатации уязвимости проходить аутентификацию не требуется
C:N	эксплуатация уязвимости не затрагивает конфиденциальные данные системы
I:P	эксплуатация уязвимости ведет к частичному нарушению целостности системы
A:N	эксплуатация уязвимости не влияет на доступность системы

Ссылки:

- Windows: http://support.microsoft.com/kb/887429
- Samba: http://lists.samba.org/archive/samba/2010-November/159265.html

172.25.1.1

500/UDP - Internet Key Exchange

Доступен агрессивный режим

Включена поддержка агрессивного режима с парольной защитой. Это позволяет злоумышленнику получить хэш пароля, а затем подобрать по нему пароль.

Решение:

Отключите агрессивный режим.

CVSS	
Базовая оценка	5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
AV:N	данная уязвимость может эксплуатироваться удаленно
AC:L	для эксплуатации уязвимости не требуются особые условия
Au:N	для эксплуатации уязвимости проходить аутентификацию не требуется
C:P	эксплуатация уязвимости влечет существенное разглашение конфиденциальных данных
I:N	эксплуатация уязвимости не затрагивает целостность системы
A:N	эксплуатация уязвимости не влияет на доступность системы

172.25.1.7 (ns1.company.local)

Linux Kernel

Не установлено обновление безопасности.

Решение:

Используйте рекомендации производителя.

Ссылки:

- CVE (CVE-2012-0207): https://www.redhat.com/security/data/cve/CVE-2012-0207.html
- CVE (CVE-2011-3638): https://www.redhat.com/security/data/cve/CVE-2011-3638.html
- CVE (CVE-2011-4086): https://www.redhat.com/security/data/cve/CVE-2011-4086.html
- CVE (CVE-2011-4127): https://www.redhat.com/security/data/cve/CVE-2011-4127.html
- CVE (CVE-2012-0028): https://www.redhat.com/security/data/cve/CVE-2012-0028.html
- CVE (CVE-2012-0207): https://www.redhat.com/security/data/cve/CVE-2012-0207.html
- CVE (CVE-2011-1083): https://www.redhat.com/security/data/cve/CVE-2011-1083.html
- CVE (CVE-2011-1083): https://www.redhat.com/security/data/cve/CVE-2011-1083.html
- CVE (CVE-2011-3347): https://www.redhat.com/security/data/cve/CVE-2011-3347.html
- CVE (CVE-2009-4067): https://www.redhat.com/security/data/cve/CVE-2009-4067.html
- CVE (CVE-2011-1160): https://www.redhat.com/security/data/cve/CVE-2011-1160.html
- CVE (CVE-2011-1585): https://www.redhat.com/security/data/cve/CVE-2011-1585.html
- CVE (CVE-2011-1833): https://www.redhat.com/security/data/cve/CVE-2011-1833.html
- CVE (CVE-2011-2484): https://www.redhat.com/security/data/cve/CVE-2011-2484.html
- CVE (CVE-2011-2496): https://www.redhat.com/security/data/cve/CVE-2011-2496.html
- CVE (CVE-2011-2695): https://www.redhat.com/security/data/cve/CVE-2011-2695.html
- CVE (CVE-2011-2699): https://www.redhat.com/security/data/cve/CVE-2011-2699.html
- CVE (CVE-2011-2723): https://www.redhat.com/security/data/cve/CVE-2011-2723.html
- CVE (CVE-2011-2942): https://www.redhat.com/security/data/cve/CVE-2011-2942.html
- CVE (CVE-2011-3131): https://www.redhat.com/security/data/cve/CVE-2011-3131.html
  - CVE (CVE-2011-3188): https://www.redhat.com/security/data/cve/CVE-2011-3188.html

6. Рекомендуемые шаги

Устранение выявленных уязвимостей

- Провести работу по устранению уязвимостей, выявленных в ходе проекта. Детальная информация по выявленным уязвимостям приведена в Отчете по результатам комплексного аудита информационных систем ИТ-инфраструктуры.

Улучшение процессов информационной безопасности и непрерывности бизнеса

- Обеспечить комплексный подходи к защите информационных активов Компании, включая не только технические аспекты обеспечение информационной безопасности, но и разработку организационно-технической документации, формирующей требования по всем областям и функциям информационной безопасности, включая управление непрерывностью и доступностью информационных систем.
- Организовать построение целостной системы управления информационной безопасности по требованиям СТО БР ИББС.
- Организовать реально функционирующее подразделение по информационной безопасности, в ответственность которого будет входить:
  - разработка организационных и технических требований к функциям ИБ и согласование требований с бизнес-подразделениями;
  - постановка задач администраторам информационных систем в соответствии с выработанными требованиями к функциям информационной безопасности;
  - контроль выполнения требований к функциям информационной безопасности и выработка рекомендаций по совершенствованию

Мониторинг и поддержка защищенности систем

- Организовать процесс управления обновлениями для программных активов.
- Организовать процесс технического мониторинга событий ИБ систем и внедрить процедуру реагирования на события информационной безопасности
- Провести инвентаризацию всех активов Банка и провести оценку рисков в соответствии с требованиями СТО БР ИББС
- Проводить регулярную независимую оценку информационной безопасности.
- Разработать пакет документов по ИБ в соответствии с требованиями СТО БР ИББС

8. Устный зачет по Теме 4

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Что такое аудит безопасности?
2. Назовите цели аудита.
3. Назовите виды аудита безопасности
4. Перечислите состав работ по проведению аудита безопасности.
5. Кто является конечным потребителем результатов аудита?
6. Как проводится инструментальный анализ защищенности?
7. Каковы особенности использования инструментальных средств для сбора информации?
8. Для чего нужен Тест на проникновение (Penetration testing)?

9. Опишите обобщенный план удаленного аудита.

Эталоны ответов: приведены в Учебном пособие по дисциплине «Правовое обеспечение информационной безопасности».

3.2. Контрольно-оценочные материалы для промежуточной аттестации по дисциплине

Формой промежуточной аттестации по учебной дисциплине является **экзамен.**
Перечень экзаменационных вопросов:

1. Порядок введения режима коммерческой тайны на предприятии
2. Порядок учета предоставления работникам информации, составляющей коммерческую тайну
3. Контроль соблюдения режима коммерческой тайны
4. Анализ организации защиты коммерческой тайны на предприятии
5. Порядок разработка перечня данных предприятия, составляющих коммерческую тайну. Содержание проекта приказа о введении режима коммерческой тайны
6. Международные стандарты в области информационной безопасности
7. Процесс создания системы защиты персональных данных в организации
8. Классификация ИСПДн в организации
9. Перечень внутренних документов организации по защите персональных данных в организации и их характеристика.
10. Мероприятия по техническому обеспечению безопасности ПДн
11. Политика безопасности предприятия: понятие, назначение, структура.
12. Политика информационной безопасности предприятия: верхний уровень
13. Политика информационной безопасности предприятия: средний уровень
14. Содержание детализированной политики безопасности
15. Политика информационной безопасности предприятия: нижний уровень
16. Аудит состояния информационной безопасности на предприятии в соответствии с ISO 17799
17. Проведение аудиторского обследования и сбор информации
18. Проверка состояния физической безопасности информационной инфраструктуры
19. Документы аудита информационной безопасности: перечень, характеристика.
20. Инструментальная проверка защищенности

Эталоны ответов представлены в Учебном пособии «Организационно-правовое обеспечение информационной безопасности».

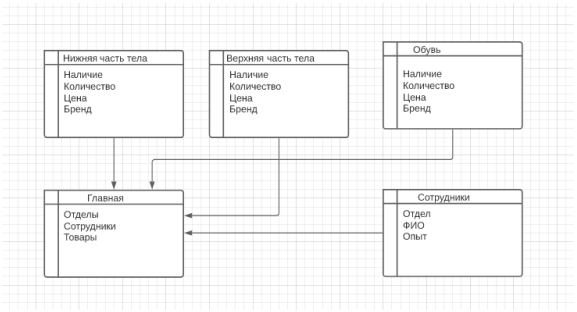
Практическая работа № 2

Выполнение прямого и обратного проектирования

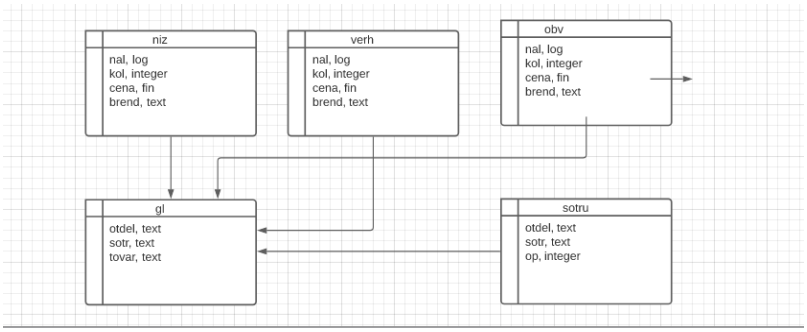
Задание.

Выполнить прямое и обратное проектирование на примере БД

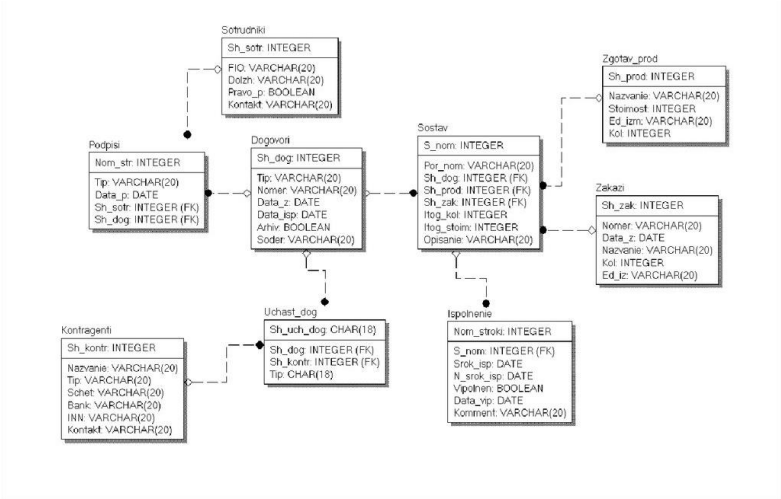
Создать логическую модель БД для магазина одежды.



Для нее прописать физическую модель.



Эталоны ответов



Устный зачет по темам 1-2

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.
Выполнение задания: одному студенту на ответ выделяется 5 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Цели, задачи, этапы и объекты анализа программного кода
2. Механизмы и контроль внесения изменений в код.
3. Обратное проектирование
4. Правовые акты, законы в области анализа программных продуктов, проведения обратного инжиниринга
5. Анализ потоков данных
6. Статический анализ кода
7. Динамический анализ кода
8. Дизассемблирование
9. Техники внедрения кода
10. Зашита программ от исследования
11. Анализ вредоносных программ

Эталоны ответов: приведены в Учебном пособии по дисциплине «Реверсивный инжиниринг».

Практическая работа №8

Создание макросов

Задание.

1. написать макрос для закрытия программы
2. написать макросы для улучшения команд PUSH и POP
3. написать макрос обнуления регистра

Эталоны ответов

1. Макрос для закрытия программы:

```
; Простой макрос без параметров, предназначенный для завершения программы
macro exit_app
{
   mov ax,4C00h
   int 21h
}
```

2. макросы для улучшения команд PUSH и POP

Макрос - улучшенная команда push

```
macro push [arg] { push arg }
```

Макрос - улучшенная команда pop

```
macro pop [arg] { pop arg }
```

3. Макрос для обнуления регистра:

```
; Макрос - команда обнуления регистра
macro clr reg { xor reg,reg }
```

Практическая работа №14

Управление клавиатурой

Задание.

Разработать программу обработки прерывания от клавиатуры, которая должна:

распознавать нажатие "горячей" комбинации клавиш и реагировать на него звуковым сигналом;

при первом нажатии "горячей" комбинации переходить в режим блокировки ввода заданной клавиши, при втором - отменять этот режим;

системная обработка всех других клавиш нарушаться не должна.

Программа должна состоять из основной программы и трех функций.

- void *readvect(int in) - функция читает вектор прерывания с номером in и возвращает его значение.
- void writevect (int in, void *h) - функция устанавливает новый вектор прерывания in на новый обработчик этого прерывания по адресу h.
- void interrupt new9() - процедура нового обработчика прерывания 9h.

Главная программа должна выполнять такие действия:

1. Запоминает адрес старого обработчика прерывания 9h, вызывая функцию readvect(in) с параметром in=9.

2. Записывает в таблицу векторов прерываний адрес нового обработчика прерывания с помощью функции writevect().

3. Вводом строки символов дает возможность проверить работу программы и ее реакцию на нажатие "горячей" комбинации клавиш и блокирование/разблокирование ввода клавиши "3".

4. В конце работы восстанавливает в таблице векторов прерываний адрес старого обработчика.

Для решения задачи процедура обработки прерывания от клавиатуры new9() должна действовать по такому алгоритму:

Эталоны ответов

```
/*-------------------Лабораторная работа N14 ---------- */
/*-------------------Управление клавиатурой ---------- */
/* Подключение стандартных заголовков */
#include <dos.h>

void interrupt (*old9)(); /* Старый обработчик прерывания 9h */
void interrupt new9();  /* Новый обработчик прерывания 9h */
void *readvect (int in);  /* Чтение вектора              */
void writevect (int in,void *h); /* Запись вектора       */

unsigned char F3_code=61; /* scan-code "F3"              */
unsigned char key3_code=4;/* scan-code "3"               */
char f=0;              /* Флаг                        */
union REGS rr;
struct SREGS sr;

/*-------------------------------------*/
void main()
{
  char string[80]; /* Буфер для ввода текста */

  textbackground(0);
  clrscr();
  textattr(0x0a);
  cprintf("----------");
  cprintf("            Лабораторная работа N14            ");
  cprintf("----------");
  cprintf(" ---------- ");
  cprintf("            Управление клавиатурой             ");
  cprintf("----------");

  old9=readvect(9);
  writevect(9,new9);
  textattr(0x0c);
  cprintf("\n\n\r\"горячая\" комбинация: ");
  textattr(0x0a);
  cprintf("Left Shift, Right Ctrl, F3\n\r");
  textattr(0x0b);
  cprintf("Клавиша, которая блокируется: ");
  textattr(0x0f);
  cprintf("3");
  textattr(0x07);
  cprintf("\r\nВводите строку символов>");
  scanf("%s",string);
  writevect(9,old9);
```

```
}
/*----------------------------------------*/
/* Чтение вектора */
void *readvect(int in)
{
  rr.h.ah=0x35;
  rr.h.al=in;
  intdosx(&rr,&rr,&sr);
  return(MK_FP(sr.es,rr.x.bx));
}
/*----------------------------------------------------------*/
/* Запись вектора */
void writevect(int in,void *h)
{
  rr.h.ah=0x25;
  rr.h.al=in;
  sr.ds=FP_SEG(h);
  rr.x.dx=FP_OFF(h);
  intdosx(&rr,&rr,&sr);
}
/*----------------------------------------*/
/* Новый обработчик 9-го прерыванмя */
void interrupt new9()
{
  unsigned char c,x,y;
  unsigned char byte17,byte18;
  unsigned char mask=0x02;
  unsigned char mask17=0x04;
  unsigned char mask18=0x01;

  byte17=peekb(0x40,0x17);
  byte18=peekb(0x40,0x18);
  if((inportb(0x60)==F3_code)&&(byte17&mask)&&
                    (byte17&mask17)&&(!(byte18&mask18)))
  {
   cputs("\7");
   x=wherex();
   y=wherey();
   gotoxy(55,3);
   textattr(0x1e);
   if(f==0)
   {
    f=1;
    cprintf("Клавиша \"3\" заблокирована ");
   }
   else
   {
    f=0;
    cprintf("Клавиша \"3\" разблокирована");
   }
   gotoxy(x,y);
   textattr(0x07);
```

```
  (*old9)();
 }
 if( (f==1) && (inportb(0x60)==key3_code) )
 {
  c=inportb(0x61);
  outportb(0x61,c|0x80);
  outportb(0x61,c);
  outportb(0x20,0x20);
 }
 else
  (*old9)();
}
```

Практическая работа №15

Управление программами

Задание.

Разработать программу, производящую форматный вывод на печать своего Префикса Программного Сегмента.

Данная программа производит распечатку основных полей своего PSP. Для этого префикс программного сегмента представим в виде следующей структуры:

```
struct psp
{       /* ФОРМАТ PSP */
  byte ret_op[2];       /* команда INT 20h              */
  word end_of_mem;      /* вершина доступной памяти     */
  byte reserved1;
  byte old_call_dos[5]; /* старый вызов DOS             */
  void *term_ptr;       /* адрес завершения             */
  void *ctrlbrk_ptr;    /* адрес обработчика Ctrl+Break */
  void *criterr_ptr;    /* адрес обработчика крит.ошибок */
  word father_psp;      /* PID родителя                 */
  byte JFT[20];         /* таблица файлов программы     */
  word env_seg;         /* адрес окружения              */
  void *stack_ptr;      /* адрес стека                  */
  word JFT_size;        /* размер таблицы файлов        */
  byte *JFT_ptr;        /* адрес таблицы файлов         */
  byte reserved2[24];
  byte new_call_dos[3]; /* новый вызов DOS              */
  } *p_psp;
```

Эталоны ответов

```
/*----------------"Управление программами"----------------*/

/* Подключение стандартных заголовков */
#include <dos.h>
#include <conio.h>

/* Типы данных */
#define byte unsigned char
```

```
#define word unsigned int

/* Описание функций */
void get_DOS_version_h(void);  /* Определение версии DOS  */
void addr_PSP (void);          /* Получение адреса PSP    */

struct psp
{       /* ФОРМАТ PSP */
  byte ret_op[2];       /* команда INT 20h               */
  word end_of_mem;      /* вершина доступной памяти      */
  byte reserved1;
  byte old_call_dos[5]; /* старый вызов DOS              */
  void *term_ptr;       /* адрес завершения              */
  void *ctrlbrk_ptr;    /* адрес обработчика Ctrl+Break  */
  void *criterr_ptr;    /* адрес обработчика крит.ошибок */
  word father_psp;      /* PID родителя                  */
  byte JFT[20];         /* таблица файлов программы      */
  word env_seg;         /* адрес окружения               */
  void *stack_ptr;      /* адрес стека                   */
  word JFT_size;        /* размер таблицы файлов         */
  byte *JFT_ptr;        /* адрес таблицы файлов          */
  byte reserved2[24];
  byte new_call_dos[3]; /* новый вызов DOS               */
  } *p_psp;

word pid;               /* сегм.адрес PSP                */
int dos_ver,            /* версия DOS                    */
    i, l, j;
char *s;
union REGS rr;

main()
{
  textbackground(0);
  clrscr();
  textattr(0x0a);
  cprintf("----------");
  cprintf("            Лабораторная  работа N16           ");
  cprintf("----------");
  cprintf(" ---------- ");
  cprintf("             Управление программами             ");
  cprintf("----------");
  textcolor(11);
  get_DOS_version_h();
  addr_PSP();
  /* распечатка PSP */
  cprintf("\n\n           Адрес PID = %04X\n\n\r",pid);
  p_psp=(struct psp *)MK_FP(pid,0);
  textcolor(10);
  cprintf("Команды:\n\r");
  cprintf(" -------\n\r");
  textcolor(14);
```

```
cprintf("     Завершение - int 20h:");
textcolor(12);
cprintf("  %02X %02X\n\r",p_psp->ret_op[0],p_psp->ret_op[1]);
textcolor(14);
cprintf("     Старый вызов DOS:      ");
textcolor(12);
for (i=0;i<5;cprintf("%02X ",p_psp->old_call_dos[i++]));
textcolor(14);
cprintf("\n\r     Новый вызов DOS:       ");
textcolor(12);
for(i=0;i<3;cprintf("%02X ",p_psp->new_call_dos[i++]));
textcolor(10);
cprintf("\n\n\rАдреса:\n\r");
cprintf(" ------ \n\r");
textcolor(14);
cprintf("    Конец памяти:             ");
textcolor(12);
cprintf("%04X:0000\n\r",p_psp->end_of_mem);
textcolor(14);
cprintf("    Обработчик завершения:    ");
textcolor(12);
cprintf("%Fp\n\r",p_psp->term_ptr);
textcolor(14);
cprintf("    Обработчик Ctrl+Break:    ");
textcolor(12);
cprintf("%Fp\n\r",p_psp->ctrlbrk_ptr);
textcolor(14);
cprintf("    Обработчик критич.ошибки: ");
textcolor(12);
cprintf("%Fp\n\r",p_psp->criterr_ptr);
textcolor(14);
cprintf("    Стек:                     ");
textcolor(12);
cprintf("%Fp\n\n\r",p_psp->stack_ptr);
textcolor(14);
cprintf("\n\rРодитель: ");
textcolor(12);
cprintf("%04X  ",p_psp->father_psp);
textcolor(0x8b);
cprintf("\n\n\rНажмите любую клавишу....\n\r\7");
getch();
clrscr();
textattr(0x0a);
cprintf("----------");
cprintf("           Лабораторная  работа N16            ");
cprintf("----------");
cprintf(" ---------- ");
cprintf("            Управление программами             ");
cprintf("----------");
/* Распечатка таблицы файлов */
s=p_psp->JFT_ptr;
textcolor(10);
```

```
  cprintf("\n\n\rТаблица файлов: ");
  textcolor(12);
  cprintf("%Fp (%d) ",s,p_psp->JFT_size);
  textcolor(11);
  if (s==(byte *)p_psp+0x18)
  cprintf(" -  в этом же PSP");
  cprintf("\n\r");
  for (i=0; ++i<=p_psp->JFT_size; cprintf("%d ",*(s++)));
  textcolor(10);
  cprintf("\n\n\rОкружение DOS: ");
  textcolor(12);
  cprintf("%04X\n\r",p_psp->env_seg);
  s=(char *)MK_FP(p_psp->env_seg,0);
  textcolor(11);
  while(l=strlen(s))
  {
    cprintf("       %s\n\r",s);
    s+=l+1;

  }
  if (dos_ver>2)
  {
    /* для DOS 3.0 и дальше можно получить строку вызова */
    s++;
    l=*((int *)s);
    textcolor(10);
    cprintf("\n\rЧисло строк вызова: ");
    textcolor(12);
    cprintf("%d\n\r",l);
    s+=2;
    textcolor(11);
    for(i=0; i<l; i++)
    {
      cprintf("%s\n\r",s);
      s+=strlen(s)+1;
    }
  }
  textattr(0x8b);
  cprintf("\n\n\n\n\rНажмите любую клавишу ...\7");
  textattr(0x07);
  cprintf("\n\r");
  getch();
  clrscr();
}

/* Определение версии DOS */
void get_DOS_version_h(void)
{
  rr.h.ah=0x30;
  intdos(&rr,&rr);
  dos_ver=rr.h.al;
}
```

```
/* Получение адреса PSP */
void addr_PSP (void)
{
  rr.h.ah=0x62;
  intdos(&rr,&rr);
  pid=rr.x.bx;
}
```

Практическая работа №16

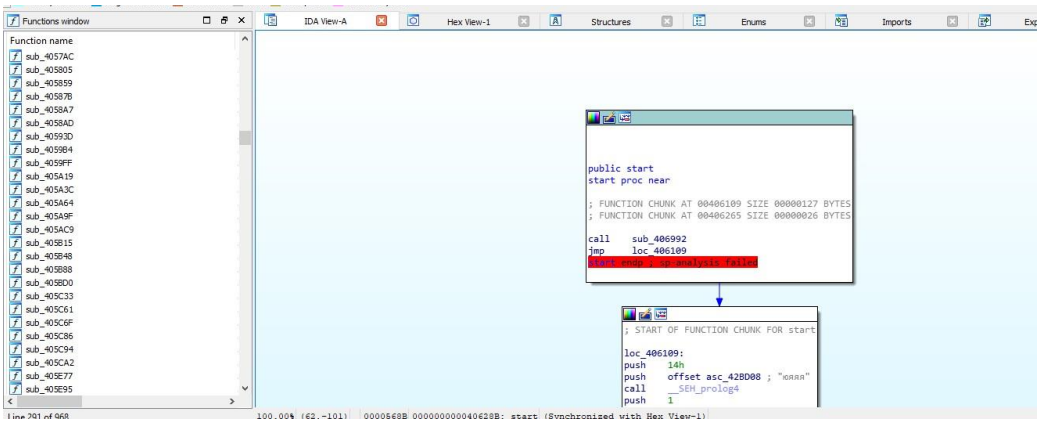
Проведение анализа вирусов используя IDA PRO

Задание.

Открыть исполняемый файл в IDA PRO

https://www.cyberforum.ru/low-level/thread1031398.html

Представлен код вируса. Изучить его:



Эталоны ответов

На что направлен вирус?

- На удаление всех exe файлов

Принцип действия вируса?

- Запускается приложение, вместе с ним запускается вирус, который начинается удаление всех exe файлов в системе

Насколько опасен этот вирус? К чему приведет его работа?

Опасность вируса заключается в том, что в системе могут храниться важные программы, которые будут удалены безвозвратно. А сами программы могут содержать в себе данные, которые приносят различную пользу владельцам или являются конфиденциальными.

Как изменить код, чтобы вирус перестал быть опасным?

Заменить или удалить основные функции в приложении, так как перестанет работать и соответственно перестанет быть вредоносным.

Либо же добавить функцию или операцию перед кодом вируса, которая будет блокировать дальнейшее выполнение кода.

Устный зачет по темам 3-5

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.
Выполнение задания: одному студенту на ответ выделяется 5 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Регистры, память и логическая адресация микропроцессора.
2. Режимы работы микропроцессора.
3. Логика, организация, компоновка, выполнение программы.
4. Защита программ от копирования и несанкционированного доступа.
5. Понятие системного программирования. Классификация системных программ.
6. Назначение и функции компиляторов и компоновщиков
7. Назначение и функции загрузчиков, трансляторов
8. Процесс выполнения программ: создание, завершение процессов и потоков.
9. Тестирование программных модулей.
10. Применение IDA PRO для обратной разработки программ

Эталоны ответов: приведены в Учебном пособии по дисциплине «Реверсивный инжиниринг».

3.2. Контрольно-оценочные материалы для промежуточной аттестации по дисциплине

Формой промежуточной аттестации по учебной дисциплине является **дифференцированный зачет**

Перечень вопросов для дифференцированного зачета:

1. Цели, задачи, этапы и объекты анализа программного кода
2. Механизмы и контроль внесения изменений в код.
3. Обратное проектирование
4. Правовые акты, законы в области анализа программных продуктов, проведения обратного инжиниринга
5. Анализ потоков данных
6. Статический анализ кода
7. Динамический анализ кода
8. Дизассемблирование
9. Техники внедрения кода

10. Зашита программ от исследования
11. Анализ вредоносных программ
12. Регистры, память и логическая адресация микропроцессора.
13. Режимы работы микропроцессора.
14. Логика, организация, компоновка, выполнение программы.
15. Защита программ от копирования и несанкционированного доступа.
16. Понятие системного программирования. Классификация системных программ.
17. Назначение и функции компиляторов и компоновщиков
18. Назначение и функции загрузчиков, трансляторов
19. Процесс выполнения программ: создание, завершение процессов и потоков.
20. Применение IDA PRO для обратной разработки программ

Эталоны ответов: приведены в Учебном пособии по дисциплине «Реверсивный инжиниринг».