Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Кубанский государственный технологический университет»
(ФГБОУ ВО «КубГТУ»)
Институт компьютерных систем и информационной безопасности
Кафедра компьютерных технологий и информационной безопасности

Отчет по практическим работам по дисциплине «Методы оценки безопасности компьютерных систем»

Выполнили студенты гр. 20-К-АС1
Сорокина А., Гращенкова А., Курышев Р.

г. Краснодар

2023

Практическое занятие №1.1 Изучение законодательства РФ в области защиты информации

Цель – для конкретного информационного объекта определить задачи, функции службы информационной безопасности

1. *Принципы службы информационной безопасности:*

- Соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ;
- Открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;
- Правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
- Приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

Функции деятельности службы:

- Проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности РФ, разрабатывает меры по её обеспечению;
- Организует работу законодательных и исполнительных органов государственной власти РФ по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности РФ;
- Поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;

- Осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
- Проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территорий РФ и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
- Способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
- Формулирует и реализует государственную информационную политику России;
- Организует разработку федеральной программы обеспечения информационной безопасности РФ, объединяющей усилия государственных и негосударственных организаций в данной области;
- Способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Организационно-правовой статус службы безопасности определяется следующим образом:

- Численность службы безопасности должна быть достаточной для выполнения всех функций;
- Служба защиты должна подчиняться тому лицу, которое в данном учреждении несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;
- Штатный состав службы безопасности не должен иметь других обязанностей, связанных с функционированием АС;
- Сотрудники службы безопасности должны иметь право доступа во все помещения, где установлена АС, и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;
- Руководителю службы безопасности должно быть предоставлено право запрещать включение в число действующих новые элементы АС, если онине отвечают требованиям защиты информации;
- Службе безопасности информации должны обеспечиваться все условия, необходимые для выполнения своих функций.

2. Разработать перечень задач для службы информационной безопасности для конкретного предприятия, сформировать список защищаемой информации, угроз безопасности информации.

Перечень задач для службы безопасности:

- Изучение технических и технологических характеристик объекта ИС и технических средств, а также организации их эксплуатации.
- Изучение системы принятых на объекте ИС мер по защите от актов незаконного вмешательства.
- Изучение способов реализации потенциальных угроз совершения актов незаконного вмешательства в деятельность объекта ИС с использованием совокупности сведений о численности, оснащенности, а также действий потенциальных нарушителей, преследуемых целей при совершении акта незаконного вмешательства в деятельность объекта.
- Определение рекомендаций субъекту ИС в отношении мер, которые необходимо дополнительно включить в систему мер по обеспечению информационной безопасности объекта или технических средств.

Список защищаемой информации:

- Информация, составляющая государственную тайну;
- Конфиденциальная информация;
- Персональные данные граждан;
- Открытые информационные ресурсы
- Автоматизированные системы управления технологическими процессами
- Государственные и муниципальные ИС

Угрозы безопасности информации:

- Внешние угрозы, исходящие от субъектов, не входящие в состав пользователей и обслуживающего персонала системы, разработчиков системы и не имеющих непосредственного контакта с информационными системами и ресурсами, а также от природных явлений, катастроф;
- Внутренние угрозы, исходящие от пользователей и обслуживающего персонала системы, разработчиком системы, других субъектов, вовлеченных в информационные процессы, и имеющих непосредственный контакт с информационными системами и ресурсами, а также при

отказах аппаратных и технических средств и сбоях программного обеспечения.

- компрометация конфиденциальной информации;

- нарушение целостности информации, включая изменения или фальсификацию, а также полное или частичное уничтожение информации;

- нарушение доступности информации, включая блокирование санкционированного доступа к информации пользователей.

Практическое занятие №1.2 Изучение правовых режимов защиты информации.

Цель – спроектировать структуру службы защиты информации

Директор – управление деятельностью системы, осуществление контроля за установкой и функционированием техники, обеспечивающей сохранность данных, организация правильного оформления технической документации, консультирование и осуществление обучение коллег в сфере ИБ, организация мероприятий по правовой и организационной защите бизнеса.

Начальник службы защиты информации – организация разработки и внедрение организационных и технических мероприятий по комплексной защите информации, обеспечивает соблюдение режима проводимых работ и сохранение конфиденциальности документированной информации, руководство проведением работ по организации, координации, методическому руководству и контролю их выполнения по вопросам защиты информации и разработки технических средств контроля, определяет перспективы их развития.

Аналитик – анализ существующей системы безопасности, на предмет угроз, определение потребности в средствах технической защиты информации.

Юрист – отвечать за документацию, отслеживать и пресекать нарушение законодательства, выстраивать сотрудничество с поставщиками, заказчиками, органами власти, использовать нормы права в интересах компании.

Сотрудники сектора обеспечения безопасности – обеспечение контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой в своей зоне ответственности, модернизация и интеграция архитектуры, обнаружение и реакция на угрозы, сохранение жизнеспособности бизнеса в случае атаки.

Сотрудники экономической разведки – сбор информации, наблюдение за конкурентами, поиск путей развития, разработка новых подходов к ведению бизнеса.

Сотрудники промышленной контрразведки – выявление субъектов передающих конфиденциальную информацию, предотвращение утечки конфиденциальной информации.

Сотрудник сектора технической защиты – выявление угроз безопасности информации, определение возможности технической разведки и проведение мероприятий технической защиты информации, участвует в категорировании объектов информатизации, выявлении угроз безопасности информации и технических каналов утечки информации, работах по проведению специальных проверок и специальных исследований объектов информатизации.

Сотрудники сектора охраны и режима – осуществляет охрану здания, помещений, оборудования, линий связи и перевозок, пожарную охрану, а также личную охрану руководящего состава.

Администратор безопасности системы – ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления и за хранением резервных копий.

Практическое занятие №1.3 Изучение организационно-правовых методов информационной безопасности.

Цель – для конкретного информационного объекта определить задачи, функции службы информационной безопасности.

1. **Определить функции отдела информационной безопасности**

- Обеспечить защиту информационных ресурсов организации от намеренного и ненамеренного разглашения, утери, искажения, похищения;
- Разработка и внедрение системы безопасности, а также контроль за её работой и анализ эффективности используемых средств защиты информации;
- Внедрение режима конфиденциальности и контроль за его соблюдением;
- Взаимодействие с контрагентами, обеспечение конфиденциальности передачи данных и информации, сообщаемой партнерам в процессе открытых переговоров;
- Разработка документов, предписывающих соблюдение режима конфиденциальности штатными сотрудниками организации и прикомандированными работниками;
- Оценка эффективности внедренной системы защиты информационных ресурсов организации от намеренного и ненамеренного разглашения, утери, искажения, похищения;
- Проведение аттестации сотрудников с последующим присвоением им необходимой степени допуска к чтению и использованию конфиденциальной информации;
- Составление актов проверки техники, оборудования, помещений на предмет их соответствия требованиям безопасности;
- Другие функции, выполнение которых поспособствует реализации целей и задач работы отдела.

2. **Перечислить общие принципы деятельности службы**

- Конфиденциальность – пользователь должен иметь право доступа только к той части информации, которая ему необходима для выполнения своих служебных обязанностей;
- Целостность – информация должна быть защищена от изменений или искажений, она должна храниться и передаваться по надежным каналам связи;
- Доступность – информация должна быть доступна пользователю по мере необходимости.

3. **Перечислить общие виды гарантий безопасности объектов защиты**

- **Нормативные гарантии** заключаются в разработке, толковании и реализации норм права, установлении пределов их действия, в формировании необходимых правоотношений, определении и обеспечении правомерного предприятия по поводу его безопасности, использовании мер государственного и административного принуждения, применении санкций к физическим лицам и юридическим лицам, посягающим на законные интересы предприятия, постоянном совершенствовании юридической технологии деятельности СБ.
- **Организационные гарантии** формируются путем разработки, построения и поддержания высокой работоспособности общей организационной структуры управления процессом выявления и подавления угроз деятельности предприятия, использование эффективного механизма её оптимального функционирования, соответствующей подготовки кадров, а также принятия мер по гармонизации интересов и консолидации усилий сотрудников предприятия на достижение целей обеспечения его безопасности;
- **Материальные гарантии** формируются за счет выделения и использования финансовых, технических, кадровых, интеллектуальных, информационных и иных ресурсов предприятия, обеспечивающих своевременное выявление, ослабление и подавление источников угрозы, предотвращение и локализацию возможного ущерба и создание благоприятных возможностей и условий деятельности предприятия.

Практическое занятие №2.1 Изучение порядка проведения лицензирования и видов деятельности предприятий в области защиты информации.

Цель – для конкретного информационного объекта определить технологию управления службой защиты информации.

1. **Определить функции отдела информационной безопасности**

- Обеспечить защиту информационных ресурсов организации от намеренного и ненамеренного разглашения, утери, искажения, похищения;
- Разработка и внедрение системы безопасности, а также контроль за её работой и анализ эффективности используемых средств защиты информации;
- Внедрение режима конфиденциальности и контроль за его соблюдением;
- Взаимодействие с контрагентами, обеспечение конфиденциальности передачи данных и информации, сообщаемой партнерам в процессе открытых переговоров;
- Разработка документов, предписывающих соблюдение режима конфиденциальности штатными сотрудниками организации и прикомандированными работниками;
- Оценка эффективности внедренной системы защиты информационных ресурсов организации от намеренного и ненамеренного разглашения, утери, искажения, похищения;
- Проведение аттестации сотрудников с последующим присвоением им необходимой степени допуска к чтению и использованию конфиденциальной информации;
- Составление актов проверки техники, оборудования, помещений на предмет их соответствия требованиям безопасности;
- Другие функции, выполнение которых поспособствует реализации целей и задач работы отдела

2. **Перечислить общие технологии информационной безопасности**

- Компонент обеспечения безопасности объектов транспортной инфраструктуры и транспортных средств предполагает идентификацию каждого объекта, его категорирование, проведение оценки уязвимости, установление требований безопасности конкретного объекта, планирование мероприятий по обеспечению его безопасности. В данном компоненте отражается мониторинг состояния объектов, а также отчеты по обеспечению его безопасности. Обязательному отражению в этой части системы подлежат внештатные ситуации, содержащие угрозы безопасности каждого конкретного объекта.

- Вторым компонентом является база данных о пассажирах. Данный компонент заключается в сборе, обработке и фиксированной информации обо всех пассажирах, участвующих как во внутренних, так и международных перевозках. Фиксирование информации производится по видам перевозок с градацией в зависимости от вида транспорта. Данные о пассажирах могут вноситься на основании сведений, предоставленных субъектами транспортной инфраструктуры, если поездка связана с пересечением государственной границы, соответствующие данные представляют федеральные органы власти, иностранными государствами и организациями. В данном случае обязанности по предоставлению сведений для базы данных о пассажирах возлагаются на органы Федеральной миграционной службы, а также ведомства, выдающие разрешение на выезд за пределы России и въезд в иностранное государство. В качестве иностранных государств выступают посольские и консульские учреждения, к ведению которых отнесены функции государства по выдаче разрешения на въезд в данное государство. Данные субъекты могут осуществлять функции по предоставлению сведений для ЕГИС в случае проведения мероприятий межгосударственного характера, а также приглашения отдельных лиц на территорию государства либо в международную организацию. Включению в систему «Транспортная безопасность» подлежат идентификационные данные о пассажире.
- Третий компонент — это интеграции баз данных, предполагающий ведение единой системы в масштабах государства, а также предоставление информации в режиме «одного окна», причем информация должна быть предоставлена единовременно в полном объеме.

3. **Выбрать наиболее подходящую технологию управления службой защиты информации**

   Управление защитой информации на предприятии должно происходить на двух уровнях:
   - в офисе
   - на удаленном доступе: материалы находятся на удаленном ресурсе, а специалисты подключаются к ним из разных точек земного шара.

Практическое занятие №2.2 Изучение перечня средств защиты информации.

Цель – провести оценку эффективности информационного обеспечения.

1. **Название –** Force
   Вид деятельности – Производство компьютеров и периферийного оборудования
   Количество руководителей – 3
   Ёмкость рынка фирмы – 557 932 500 руб.
   Основные конкуренты – АО «компания Мирекс», GCR.
   Базы наблюдений и источники информации – Востребованность населения в продукции, рост или снижение ежемесячных продаж, и т.д.
2. **Стратегическая** – Тенденции по странам, технологический процесс (сырье, производственные технологии), действующие лица (конкуренты, партнеры, кадры), диверсификация.
   Тактическая – Основные области деятельности и виды продукции, зоны и территории деятельности, производственные мощности и способ производства, патентная и лицензионная активность.
   Оперативная – конкуренты и их коммерческая политика (ассортимент продукции, цены, рекламные компании, поставщики, клиенты, система торговли, субподрядчики)
3. Каналы распределения продукции, торговые агенты, поставщики и потребители продукции, рекламные агентства, маркетинговые фирмы, специальные аналитические службы.
4. 4 788 808,32

1. Потребительские свойства, цена, жизненный цикл.
2. Технологическая информация, деловая информация.
3. Выбрать базы наблюдения, которые предопределяются поставленными целями.
4. Стратегическая предопределяет все последующие действия.
   Тактическая заключается в выборе наилучшего средства достижения цели в контроле неизменности условий, которые предопределяют выбор.
   Оперативная обеспечение движения вперед в наилучших условиях.
5. ССПИ в рамках централизованной организованной структуры.
   СТОИ в рамках децентрализованной организованной структуры.
6. Текст, фирма, консультант, беседа, джокер.
7. Для органов управления результатом является управленческое решение, и чем выше его эффективность, тем лучше работает служба информирования, способствующая его принятию.

Практическое занятие №2.3 Изучение программно-технических методов защиты.

Цель – проанализировать состав и характеристику организации информационно-аналитической работы.

1. **Главной целью информационно-аналитической работы является создание на базе собираемых сведений и материалов обобщенной информации.**
   Основные задачи информационно-аналитической работы:
   - Обеспечить своевременное поступление надежной и всесторонней информации по интересующим вопросам;
   - Описать сценарии действий конкурентов, которые могут затрагивать текущие интересы предприятия;
   - Осуществлять постоянный мониторинг событий во внешней среде и на рынке, которые могут иметь значение для интересов предприятия;
   - Обеспечить безопасность собственных информационных ресурсов;
   - Обеспечить эффективность и исключить дублирование при сборе, анализе и распространении информации.
2. **Направление аналитической работы** определяются с учетом конкретных особенностей предприятия. К основным направлениям можно отнести анализ объекта защиты, угроз, каналов несанкционированного доступа к информации, комплексной безопасности предприятия, нарушение режима конфиденциальности, анализ подозрений утраты конфиденциальной информации.
   Постоянные направления аналитической работы являются наиболее важными. Периодические и разовые работы характеризуются своей жестокой зависимостью от постоянных направлений.
   Периодические направления проводятся через определенные промежутки времени с целью контроля эффективности и возможности внесения улучшений в действующую в фирме систему защиты информации.
   Разовые направления бывают вызваны чрезвычайными обстоятельствами и требуют проведения исследования в кротчайшие сроки.
3. **Этапы выполнения информационно-аналитических исследований производственных ситуаций:**
   1. **Заключение**. Здесь должны содержаться ответы на вопросы, какова степень важности полученной информации, её значение для принятия конкретных решений, идет ли речь о каких-либо угрозах, подозрениях, выявленных негативных факторов, какое

отношение имеет предмет отчета к другим областям аналитической работы.

2. **Рекомендации.** В этом разделе должны быть указаны конкретные направления дальнейших действий службы безопасности и других структурных подразделений предприятия для улучшения системы безопасности, предотвращения утраты информации, принятия наиболее эффективных решений.
3. **Обобщение информации.** Здесь излагают самую существенную информацию без излишней детализации.
4. **Источники и надежность информации.** В этом разделе должны быть указаны предполагаемые оценки надежности данных и источника на момент написания отчета.
5. **Основные и альтернативные гипотезы.** Обязательно должны указываться рассмотренные в ходе анализа наиболее вероятные гипотезы, что помогает принимать более взвешенные и адекватные решения, а также позволяет еще раз оценить правильность выбранной гипотезы.
6. **Недостающая информация.** Четко указывается, какая именно дополнительная информация необходима для подтверждения окончательной гипотезы и принятия решения.

4. **Методы выполнения аналитических исследований:** сравнение показателей, расчленение общих показателей на составные части, группировка и обобщение показателей, балансовый и корреляционный методы.
    - С помощью **диаграмм связей** выявляется наличие связи между субъектами, вовлеченными в конкретную ситуацию, подвергающуюся анализу, а также области общения, соприкосновения этих субъектов.
    - **Матрицы связей** отражают частоту взаимодействия субъектов ха определенный период времени. Такой метод дополняет диаграммы связей, позволяет оценить характер взаимодействия между субъектами через частоту таких взаимодействий.
    - **Схемы потоков** информации позволяют оценить то, каким образом происходят события.
    - **Временные графики** используются для регистрации событий.
    - **Экспертные системы** представляют собой класс компьютерных программ, которые выдают советы, проводят анализ, выполняют классификацию.

Практическое занятие №3.1 Изучение криптографических методов защиты.

Цель – для конкретного информационного объекта определить методы оргпроектирования деятельности службы защиты информации.

1. Функции отдела информационной безопасности организации:
   - Разработка комплексной системы безопасности, включающей использование разнообразных методов и способов защиты информации;
   - Внедрение режима конфиденциальности и контроль за его соблюдением;
   - Взаимодействие с контрагентами, обеспечение конфиденциальной передачи данных и информации, сообщаемой партнерам в процессе открытых переговоров;
   - Разработка документов, предписывающих соблюдение режима конфиденциальности штатными сотрудниками организации и прикомандированными работниками;
   - Оценка эффективности внедренной системы защиты информационных ресурсов организации от разглашения, утери, искажения, похищения;
   - Проведение аттестации сотрудников с последующим присвоением им необходимой степени допуска к чтению и использованию конфиденциальной информации;
   - Составление актов проверки техники, оборудования, помещений на предмет их соответствия требованиям безопасности;
   - Другие функции, выполнение которых поспособствует реализации целей и задач работы отдела.

2. **Общие технологии управления службой защиты информации:**
   Управление защитой информации на предприятии должно происходить на двух уровнях:
   - В офисе;
   - На удаленном доступе. (материалы находятся на удаленном ресурсе, а специалисты подключаются к ним из разных точек земного шара.)
3. **Технология управления службой защиты информации для предприятия**
   Общие ориентиры для действий:
   - Сохранение и наращивание ресурсного потенциала;
   - Проведение комплекса превентивных мероприятий по повышению уровня защищенности собственности персонала предприятия;
   - Включение в деятельность по обеспечению безопасности предприятия всех сотрудников;
   - Профессионализм и специализация персонала предприятия;

- Приоритетность не силовых методов предотвращения и нейтрализация угроз.

Типы стратегий безопасности:

- Ориентированные на устранение существующих или предотвращение возникновения возможных угроз;
- Нацеленные на предотвращение воздействия существующих или возможных угроз на предмет безопасности;
- Направленные на восстановление наносимого ущерба.

Обеспечением безопасности предприятия занимаются две группы субъектов. Первая группа занимается этой деятельностью непосредственно на предприятии и подчинены руководству. Ко второй группе субъектов относятся внешние органы и организации, которые функционируют самостоятельно и не подчиняются руководству предприятия.

Практическое занятие №3.2 Положения «Оранжевой книги» в области оценки состояния защищенности систем.

Цель – разработать пакет нормативных документов, необходимых для работы службы защиты информации вашей организации.

1. Перечислить документы необходимые для обеспечения полноценной организационной и правовой защиты информации.

1. Положения:
   - О защите персональных, секретных, конфиденциальных сведений;
   - О правилах пользования внутренней информационной сетью, использования интернет-ресурсов.
2. Распоряжения:
   - О назначении ответственных лиц по обеспечению безопасности обработки персональных данных;
   - О правилах хранения электронных и бумажных носителей ценных сведений, определения порядка допуска к ним;
   - О создании комиссии, которая занимается классификацией системы и присваивает ей соответствующий класс защиты.
3. Должностные инструкции специалистов, ответственных за программное обеспечение, работу технических средств, контролирующих доступность сведений.
4. Модель угроз безопасности, составленную на основе анализа.
5. Утвержденный список лиц с доступом к информации, имеющей стратегическое значение.
6. Правила:

- Проведения процедуры идентификации пользователей;
- Установки программного обеспечения;
- Резервирования баз данных, их восстановления при возникновении нештатных ситуаций.

7. Формы журналов учета:
   - Приема\выдачи съемных носителей данных;
   - Технических средств для обработки и передачи информации;
   - Проведение инструктажей по вопросам защиты данных, безопасного пользования персональными компьютерами;
   - Тестирования средств, обеспечивающих конфиденциальность, защиту информации;
   - Плановых мероприятий, проводимых с целью предотвращения хищений, несанкционированного доступа к секретной информации, выявления потенциальных угроз.

2. Дополнения необходимых документов, затрагивающих вопросы, связанные с защитой информации.

1. Конституция РФ (12 декабря 1993 г.)
   - Ст.24 Органы государственной власти и местного самоуправления должны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими права и свободы;
   - Ст.41 Гарантирует право на значение факторов и обстоятельств, создающих угрозу здоровью и жизни людей;
   - Ст.42 Гарантирует право на знание достоверной информации о состоянии окружающей среды;
   - Ст.23 Гарантирует право на личную и семейную тайну, на тайну переписки, телефонных разговоров, почтовых, телеграфных и иных сообщений;
   - Ст.29 Право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.
2. Гражданский кодекс РФ (15 мая 2001 г.)
   Ст.139 Информация составляет служебную или коммерческую тайну, если она имеет коммерческую ценность, к ней нет свободного доступа и обладатель информации принимает меры к охране её конфиденциальности.
3. Уголовный кодекс РФ
   - Гл.28 «Преступление в сфере компьютерной информации»

- Ст.272 «Неправомерный доступ к компьютерной информации»
- Ст.273 «Создание, использование и распространение вредоносных программ для ЭВМ»
- Ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сетей»
- Ст. 138
- Ст. 183

3. Документы необходимые для работы службы безопасности организации.

1.Положения:

- О защите персональных, секретных, конфиденциальных сведений;
- О правилах пользования внутренней информационной сетью, использования интернет-ресурсов.

2.Распоряжения:

- О назначении ответственных лиц по обеспечению безопасности обработки персональных данных;
- О правилах хранения электронных и бумажных носителей ценных сведений, определения порядка допуска к ним;
- О создании комиссии, которая занимается классификацией системы и присваивает ей соответствующий класс защиты.

3.Должностные инструкции специалистов, ответственных за программное обеспечение, работу технических средств, контролирующих доступность сведений.

4.Модель угроз безопасности, составленную на основе анализа.

5.Утвержденный список лиц с доступом к информации, имеющей стратегическое значение.

6.Правила:

- Проведения процедуры идентификации пользователей;
- Установки программного обеспечения;
- Резервирования баз данных, их восстановления при возникновении нештатных ситуаций.

7.Формы журналов учета:

- Приема\выдачи съемных носителей данных;
- Технических средств для обработки и передачи информации;
- Проведение инструктажей по вопросам защиты данных, безопасного пользования персональными компьютерами;
- Тестирования средств, обеспечивающих конфиденциальность, защиту информации;

- Плановых мероприятий, проводимых с целью предотвращения хищений, несанкционированного доступа к секретной информации, выявления потенциальных угроз.

Практическое занятие №3.3 Российские нормативно-правовые акты в области оценки состояния защищенности систем.

Цель – разработать организационно-нормативных документов, регламентирующих деятельность службы защиты информации, её подразделений и сотрудников.

1. Перечислите документы, необходимые для обеспечения полноценной организационно правовой защиты информации.

1. Положения:

- О защите персональных, секретных, конфиденциальных сведений;
- О правилах пользования внутренней информационной сетью, использования интернет-ресурсов.

2. Распоряжения:

- О назначении ответственных лиц по обеспечению безопасности обработки персональных данных;
- О правилах хранения электронных и бумажных носителей ценных сведений, определения порядка допуска к ним;
- О создании комиссии, которая занимается классификацией системы и присваивает ей соответствующий класс защиты.

3.Должностные инструкции специалистов, ответственных за программное обеспечение, работу технических средств, контролирующих доступность сведений.

4.Модель угроз безопасности, составленную на основе анализа.

5.Утвержденный список лиц с доступом к информации, имеющей стратегическое значение.

6.Правила:

- Проведения процедуры идентификации пользователей;
- Установки программного обеспечения;
- Резервирования баз данных, их восстановления при возникновении нештатных ситуаций.

7.Формы журналов учета:

- Приема\выдачи съемных носителей данных;
- Технических средств для обработки и передачи информации;

- Проведение инструктажей по вопросам защиты данных, безопасного пользования персональными компьютерами;
- Тестирования средств, обеспечивающих конфиденциальность, защиту информации;
- Плановых мероприятий, проводимых с целью предотвращения хищений, несанкционированного доступа к секретной информации, выявления потенциальных угроз.

2. Приведите примеры дополнений необходимых документов, затрагивающих вопросы, связанные с защитой информации.

1.Конституция РФ (12 декабря 1993 г.)

- Ст.24 Органы государственной власти и местного самоуправления должны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими права и свободы;
- Ст.41 Гарантирует право на значение факторов и обстоятельств, создающих угрозу здоровью и жизни людей;
- Ст.42 Гарантирует право на знание достоверной информации о состоянии окружающей среды;
- Ст.23 Гарантирует право на личную и семейную тайну, на тайну переписки, телефонных разговоров, почтовых, телеграфных и иных сообщений;
- Ст.29 Право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

2.Гражданский кодекс РФ (15 мая 2001 г.)

Ст.139 Информация составляет служебную или коммерческую тайну, если она имеет коммерческую ценность, к ней нет свободного доступа и обладатель информации принимает меры к охране её конфиденциальности.

3.Уголовный кодекс РФ

- Гл.28 «Преступление в сфере компьютерной информации»
- Ст.272 «Неправомерный доступ к компьютерной информации»
- Ст.273 «Создание, использование и распространение вредоносных программ для ЭВМ»
- Ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сетей»
- Ст. 138
- Ст. 183

3. Документы необходимые для работы службы безопасности, вашей организации.

1. Положения:

- О защите персональных, секретных, конфиденциальных сведений;
- О правилах пользования внутренней информационной сетью, использования интернет-ресурсов.

2. Распоряжения:

- О назначении ответственных лиц по обеспечению безопасности обработки персональных данных;
- О правилах хранения электронных и бумажных носителей ценных сведений, определения порядка допуска к ним;
- О создании комиссии, которая занимается классификацией системы и присваивает ей соответствующий класс защиты.

3.Должностные инструкции специалистов, ответственных за программное обеспечение, работу технических средств, контролирующих доступность сведений.

4.Модель угроз безопасности, составленную на основе анализа.

5.Утвержденный список лиц с доступом к информации, имеющей стратегическое значение.

6.Правила:

- Проведения процедуры идентификации пользователей;
- Установки программного обеспечения;
- Резервирования баз данных, их восстановления при возникновении нештатных ситуаций.

7.Формы журналов учета:

- Приема\выдачи съемных носителей данных;
- Технических средств для обработки и передачи информации;
- Проведение инструктажей по вопросам защиты данных, безопасного пользования персональными компьютерами;
- Тестирования средств, обеспечивающих конфиденциальность, защиту информации;
- Плановых мероприятий, проводимых с целью предотвращения хищений, несанкционированного доступа к секретной информации, выявления потенциальных угроз.