ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник

С. Войцеховский

«___» _____ 2022 г.

Практическое занятие № 14
по учебной дисциплине
«Защита информации»
на тему:

«Защита разработанной комплексной системы информационной безопасности АС в зависимости от задания преподавателя»

Рассмотрено и одобрено
на заседании кафедры № 27
« ___ » _____ 202_ г. протокол № ___

Санкт-Петербург
2022

I. ТЕМА И ЦЕЛЬ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Тема практического занятия: «Защита разработанной комплексной системы информационной безопасности АС в зависимости от задания преподавателя».

Цель работы: защита в ходе дскусии комплексной системы обеспечения информационной безопасности АС.

Время - 180 мин.

Место – аудитория (класс) по расписанию занятий.

Учебно-материальное и методическое обеспечение

1. Лабораторные установки – персональные ЭВМ с установленным на них программным обеспечением.
2. Методические разработки по настройки СЗИ.
3. Методическая разработка для проведения практического занятия.

II. УЧЕБНЫЕ ВОПРОСЫ И РАСЧЕТ ВРЕМЕНИ

№ п\п	Учебные вопросы	Время, мин.
1.	Вступительная часть. Контрольный опрос.	10
2.	Учебные вопросы. ОСНОВНАЯ ЧАСТЬ: 1. Разработка плана используемых ресурсов и средств для обеспечения информационной безопасности АС. 2. Настройка используемых программных средств обеспечения информационной безопасности АС. 3. Составление отчёта о проделанной работе.	 40 80 40
3.	Заключительная часть. Задание и методические указания курсантам на самостоятельную подготовку	10

УЧЕБНЫЕ МАТЕРИАЛЫ

1. Сведения из теории

Важнейшими условиями обеспечения безопасности являются законность, достаточность, соблюдение баланса интересов личности и организации, высокий профессионализм представителей службы информационной безопасности, подготовка пользователей и соблюдение ими всех установленных правил сохранения конфиденциальности, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами.

Без соблюдения этих условий никакая система информационной безопасности не может обеспечить требуемого уровня защиты.

Комплексная система защиты информации должна быть:

- централизованной; необходимо иметь в виду, что процесс управления всегда централизован, в то время как структура системы, реализующей этот процесс, должна соответствовать структуре защищаемого объекта;
- плановой; планирование осуществляется для организации взаимодействия всех подразделений объекта в интересах реализации принятой политики безопасности; каждая служба, отдел, направление разрабатывают детальные планы защиты информации в сфере своей компетенции с учетом общей цели организации;
- конкретной и целенаправленной; защите подлежат абсолютно конкретные информационной ресурсы, могущие представлять интерес для конкурентов;
- активной; защищать информацию необходимо с достаточной степенью настойчивости и целеустремленности. Это требование предполагает наличие в составе системы информационной безопасности средств прогнозирования, экспертных систем и других инструментариев, позволяющих реализовать наряду с принципом “обнаружить и устранить” принцип “предвидеть и предотвратить”;
- надежной и универсальной, охватывать весь технологический комплекс информационной деятельности объекта; методы и средства защиты должны надежно перекрывать все возможные каналы утечки информации и противодействовать способам несанкционированного доступа независимо от формы представления информации, языка ее выражения и вида носителя, на котором она закреплена;
- нестандартной (по сравнению с другими организациями), разнообразной по используемым средствам;

- открытой для изменения и дополнения мер обеспечения безопасности информации;
- экономически эффективной; затраты на систему защиты не должны превышать размеры возможного ущерба.

Наряду с основными требованиями существует ряд устоявшихся рекомендаций, которые будут не бесполезны создателям систем информационной безопасности:

- средства защиты должны быть просты для технического обслуживания и “прозрачны” для пользователей;
- каждый пользователь должен иметь минимальный набор привилегий, необходимых для работы;
- возможность отключения защиты в особых случаях, например, когда механизмы защиты реально мешают выполнению работ;
- независимость системы защиты от субъектов защиты;
- разработчики должны предполагать, что пользователи имеют наихудшие намерения (враждебность окружения), что они будут совершать серьезные ошибки и искать пути обхода механизмов защиты;
- отсутствие на предприятии излишней информации о существовании механизмов защиты.

Все перечисленные позиции должны лечь в основу формирования системы защиты информации.

При обеспечении информационной безопасности существует два аспекта:

- формальный, связанный с определением критериев, которым должны соответствовать защищаемые информационные технологии;
- практический, характеризующий порядок определения конкретного комплекса мер безопасности применительно к рассматриваемой информационной технологии.

3.Пример разработки КСИБ

ПЛАН МЕРОПРИЯТИЙ ПО ЗАЩИТЕ СЛУЖЕБНОЙ ИЛИ КОММЕРЧЕСКОЙ ТАЙНЫ ОРГАНИЗАЦИИ НА 20_ г.

Цели и задачи, принципы построения и требования к системе защиты информации

Облик будущей системы информационной безопасности

Основные этапы создания системы информационной безопасности	Результаты действий на этапах создания системы информационной безопасности
1. Выявление информации, представляющей интеллектуальную собственность организации.	Список сведений, составляющих коммерческую тайну, и организаций (частных лиц), которых эти сведения могут интересовать
2. Определение границ управления информационной безопасностью.	Инфологическая модель объекта с выявлением возможных точек нападения
3. Анализ уязвимости: - каналы утечки и НСД, - вероятность реализации угроз (установления информационного контакта), - модель действий нарушителя, - оценка ущерба (потерь).	Сценарий осуществления противоправных действий Ранжирование угроз по вероятности их осуществления и возможному ущербу Принятие стратегии управления рисками
4. Выбор контрмер, обеспечивающих информационную безопасность.	Правовые, организационные и инженерно-технические мероприятия. Определение политики безопасности
5. Проверка системы защиты информации: - оценка эффективности вариантов построения, - тестирование системы.	Формирование системы информационной безопасности на основе результатов оценки эффективности и тестирования
6. Составление плана защиты.	Пакет документов по построению системы информационной безопасности и реализации политики безопасности
7. Реализация плана защиты информации.	Монтаж и настройка оборудования, управление системой защиты

1. Цели плана по защите служебной или коммерческой тайны.

Ими могут быть:

- предотвращение несанкционированного распространения служебных, коммерческих или конфиденциальных секретов;
- предотвращение разглашения служебных или коммерческих секретов сотрудниками и другими носителями таких секретов, а также исключение утечки по техническим каналам.

2. Анализ сведений, составляющих служебную или коммерческую тайну:

- определить, какие сведения организации могут быть отнесены к служебной или коммерческой тайне;
- установить места их разработки, накопления и хранения;
- выявить потенциальные каналы утечки таких сведений;
- оценить возможности по перекрытию этих каналов;
- проанализировать соотношение затрат и доходов по использованию различных технологий, обеспечивающих защиту служебной или коммерческой тайны;
- назначить сотрудников, ответственных за каждый участок системы обеспечения безопасности.

3. Обеспечить реализацию деятельности системы безопасности по следующим направлениям:

- контроль сооружений и оборудования организации, обеспечение безопасности производственных и конторских помещений, охрана фото- и иного копировального оборудования, контроль посещений организации и т. д.;
- разработка памятки о сохранении служебной или коммерческой тайны, определение порядка ознакомления с ней, а также с Перечнем сведений, составляющих такие тайны;
- работа с персоналом организации, в том числе проведение бесед при приеме на работу, инструктаж вновь принятых на работу по правилам и процедурам защиты служебной или коммерческой тайны
- в организации, получение от них обязательств (контрактов) о неразглашении, обучение сотрудников правилам сохранения служебных и коммерческих секретов, стимулирование соблюдения конфиденциальности, беседы с увольняющимися и получение от них подписок;
- организация работы с конфиденциальными документами, установление порядка и правил ведения делопроизводства, контроль за конфиденциальными документами и их публикациями, контроль и учет техниче-

ских носителей конфиденциальных сведений, засекречивание, рассекречивание и уничтожение конфиденциальных документов, охрана чужих секретов;

- работа с конфиденциальной информацией, циркулирующей в технических средствах и системах обеспечения производственной и трудовой деятельности (создание системы защиты технических каналов защиты утечки информации);
- работа с конфиденциальной информацией, накопленной в компьютерных системах (создание системы защиты электронной информации от несанкционированного доступа к ней; обеспечение контроля за работой пользователей на ПЭВМ);
- защита служебной или коммерческой тайны в организационно-правовых вопросах и особенно в процессе заключения контрактов и договоров с коллективом, сотрудниками, смежниками, поставщиками и т. д.

4. Общие методические указания курсантам (слушателям) по подготовке к практическим занятиям

Практические занятия по дисциплине «Защита информации» проводятся в классе ПЭВМ. Индивидуальные задания выполняются каждым курсантом лично.

Перед выполнением задания обучающийся изучает материал, приведенный в разделе «Учебные материалы», в ходе которого необходимо разобрать приведенные примеры и выполнить задания раздела. На следующем этапе работы обучающийся выполняет индивидуальное задание.

Результаты работы оформляются в виде отчета. Содержание отчета приведено в руководстве по соответствующему практическому занятию.

По готовности к защите работы курсант (слушатель) докладывает преподавателю.

5. Задание к практическому занятию

ЗАДАНИЕ

Разработать систему информационной безопасности как организованную совокупность органов, средств, методов и мероприятий, обеспечивающих защиту информации от разглашения, утечки и несанкционированного доступа к ней.

Цель работы: приобрести практические навыки по разработке комплексной системы обеспечения информационной безопасности АС.

Задания за практическую работу

1. Разработка плана используемых ресурсов и средств для обеспечения информационной безопасности АС.
2. Настройка используемых программных средств обеспечения информационной безопасности АС.
3. Составление отчёта о проделанной работе.

Подготовка к работе

Подготовка к работе проводится в часы самоподготовки.

В ходе её каждый курсант обязан:

1. Изучить настоящее задание.

2. Изучить необходимую литературу для разработки комплексной системы безопасности АС.

6. Методические указания

1. В классе ПЭВМ курсанты самостоятельно под руководством преподавателя выполняют п. 5 настоящего задания. Курсанты, которые успешно справились с основным заданием, завершили оформление отчета о работе и представили его для проверки преподавателю, допускаются к защите работы.

Основные определения и справочную информацию необходимо занести в конспект.

2. При освоении приемов создания и настройки ученых записей и групп пользователей имена и прочие данные использовать любые. По окончании работы все созданные учетные записи и рабочие группы необходимо удалить!

3. Основные шаги по созданию и настройке учетных записей необходимо занести в отчет.

4. Дополнительное задание – изучить и законспектировать.

7.Отчетность по работе

По выполнению работы каждый курсант должен представить отчет. Отчет должен содержать:

– название практического занятия;

– текст индивидуального задания;

– цель работы;

– результаты проделанной работы;

– Выводы.

В процессе выполнения индивидуального задания или после завершения его выполнения преподаватель проводит собеседование с каждым курсантом по теме выполненной работы, проверяя также практические навыки, приобретенные в ходе занятия. Отчетный материал предоставляется преподавателю, а результаты защищаются.

8. Заключительная часть

В заключительной части подводятся итоги проделанной работы, дается краткая оценка действиям участников, прослеживается связь с теоретическими положениями и перспективой на будущую деятельность.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПРЕПОДАВАТЕЛЮ ПРИ ПРОВЕДЕНИИ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Во вступительной части занятия производится контроль присутствия и готовности обучающихся к занятию. Объявляется тема, цель, учебные вопросы занятия и особенности его проведения.

Готовность группы к занятию проверяется контрольным опросом.

1. Перечислите основные требования, предъявляемые к комплексной системе защиты информации.

2. Перечислите последовательность действий при разработке комплексной системы обеспечения информационной безопасности объекта.

3. Перечислите основные мероприятия, которые можно отнести к «разовым мероприятиям» построения КСИБ.

4. Перечислите основные мероприятия, которые можно отнести к «периодически проводимым мероприятиям» построения КСИБ.

5. Перечислите основные мероприятия, которые можно отнести к «мероприятиям, проводимым по необходимости» для построения КСИБ.

6. Перечислите основные мероприятия, которые можно отнести к «постоянно проводимым мероприятиям» для построения КСИБ.

7. Отвечаю на вопросы по теме занятия, даю задание на самоподготовку.

При отработке первого вопроса занятия основное внимание обратить на разработке плана используемых ресурсов и средств для обеспечения информационной безопасности АС.

При отработке второго вопроса отметить необходимость и важность настройки используемых программных средств обеспечения информационной безопасности АС.

При отработке третьего вопроса занятия основное внимание обратить на важности разработки отчета о проделанной работе.

В заключительной части занятия подвести итоги, оценить действия обучающихся, ответить на вопросы.

Дать задание на самоподготовку. Объявить тему следующего занятия.

Задание и методические указания курсантам на самостоятельную подготовку:

1. Повторить по конспекту лекций и рекомендованной литературе.
2. Быть готовыми к самостоятельной разработке КСИБ.

V. ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. План-конспект.
2. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
3. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах./ Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.
4. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Доцент 27 кафедры
к.т.н.
подполковник

С. Краснов

«___»_____20__г.