Вводная лекция

С.А. Краснов

Введение

# Введение

Вводная лекция.

Тема лекции: Введение.

## Введение

**Учебные вопросы**:

1. Цели, задачи, контрольные мероприятия по изучаемой дисциплине
2. Основные аспекты комплексного подхода обеспечения информационно-компьютерной безопасности

**Наименование направления (специальности) -** 09.04.01 Информатика и вычислительная техника - каф.ИБ (ФКТИ)

**Наименование плана направления (специальности):** 09.04.01-Информатика и вычислительная техника.

**Название дисциплины:** «Аппаратно-программные средства защиты информации в компьютерных системах».

**Название программы (профиля, специализации)** - Безопасность и этика искусственного интеллекта.

**Разработчик:** доцент, к.т.н., С.А. Краснов;

**Обеспечивающий факультет:** ФКТИ;

**Обеспечивающая кафедра:** «Информационной безопасности»;

**Общая трудоемкость –** 4 з.ед;

**Виды занятий (академ. часов):**

1. Лекции – 17 (8 лекций)
2. Практические занятия – 34 (8 ПЗ)
3. Самостоятельная работа, включая часы на контроль ¬ 93

**Все аудиторные занятия:** 51 (8 Л.+8 ПЗ.);

**Всего:** 144 (51 (Л, ПЗ) + 93(СР)).

**Вид промежуточной аттестации:** экзамен на 2 курсе в 3 семестре.

Дисциплина формирует знания, умения и навыки необходимые для защиты информации в компьютерных системах с применением современных аппаратно-программных средств защиты информации. В рамках дисциплины изучаются следующие основные темы: Основные понятия программно-аппаратной защиты информации, принципы её построения. Задачи программно-аппаратной защиты информации. Нормативные документы, посвященные вопросам применения программно-аппаратных средств защиты информации. Методы и средства защиты информации от НСД. Идентификация и аутентификация пользователей. Разграничение доступа. Доверенная загрузка. Изолированная программная среда. Программно-аппаратные механизмы защиты ОС специального назначения. Механизмы защиты сертифицированных антивирусных средств. Практические часть курса, в составе практических работ, нацелена на закрепление материала и получение навыков по настройке аппаратно-программных средств защиты информации по определенным правилам, установленным нормативными или нормативно-методическими документами.

**Цель освоения дисциплины направлена на** изучение моделей и методов информационной безопасности, требуемых при проектировании и разработке различных систем на основе технологий искусственного интеллекта и приобретение навыков для решения профессиональных задач в различных сферах деятельности.

**Основными задачами изучения дисциплины являются:**

* формирование комплексных знаний об основных тенденциях развития технологий искусственного интеллекта, связанных с обеспечением информационной безопасности;
* формирование практических навыков применения средств защиты информации, использующих технологии систем искусственного интеллекта, при решении профессиональных задач.

**В результате освоения дисциплины обучающийся будет знать** основные методы и технологии в области защиты информации, использующие технологии искусственного интеллекта, применяемые в аппаратно-программных средствах защиты информации, а также направления и перспективы их развития.

**Результатом освоения дисциплины является приобретения умений** по настройке механизмов защиты информации, в том числе основанных на технологиях искусственного интеллекта в аппаратно-программных средствах защиты информации с учетом требований информационной безопасности в различных предметных областях

**Результатом освоения дисциплины является приобретение практических навыков** учета всесторонних негативных воздействий злоумышленника на компьютерные системы при разработке, модернизации и администрирование аппаратно-программных средств защиты информации, в том числе основанных на технологиях систем искусственного интеллекта, с учетом требований информационной безопасности в различных предметных областях.

## Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Машинное обучение»
2. «Криптография и криптографические протоколы»
3. «Машинное обучение в приложениях биометрии»
4. «Представление знаний в системах искусственного интеллекта»
5. «Управление разработкой промышленного программного обеспечения» и обеспечивает подготовку выпускной квалификационной работы.

**Критерии оценивания:** формой промежуточной аттестации является экзамен.

**Неудовлетворительно:** оценка выставляется студенту, продемонстрировавшему существенные пробелы в знаниях основного учебного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий.

**Удовлетворительно:** оценка выставляется студенту, продемонстрировавшему знание основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, предусмотренных программой, обладающему необходимыми знаниями, но допустившему неточности в ответах на аттестационном испытании и при выполнении учебных заданий.

**Хорошо:** оценка выставляется студенту, продемонстрировавшему полное знание учебного материала, успешно выполнившему предусмотренные программой задачи, освоившему основную рекомендованную литературу, показавшему систематический характер знаний по дисциплине и способному к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности.

**Отлично:** оценка выставляется студенту, продемонстрировавшему всестороннее систематическое знание учебного материала, умение свободно выполнять практические задания, освоившему основную литературу и ознакомившемуся с дополнительной литературой, рекомендованной рабочей программой дисциплины, усвоившему взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившему творческие способности в понимании, изложении и использовании учебного материала.

**Особенности допуска:** К сдаче экзамена допускаются обучающиеся, выполнившие все требования учебной программы: прошедшие контрольные точки (4 коллоквиума по темам изучаемой дисциплины), выполнившие и защитившие все практические работы. Экзамен проводится в устной форме по билетам, содержащим два теоретических вопроса и практическую задачу. Совокупность оценок, полученных студентом в результате контрольных мероприятий, учитывается преподавателем при проведении промежуточной аттестации в форме экзамена. При этом оценка по результатам текущего контроля составляет 60% от общей итоговой оценки, экзаменационная ¬40%.

Со списком литературы, необходимым для качественного изучения данной дисциплины, можно ознакомиться в рабочей программе дисциплины «Аппаратно-программные средства защиты информации в компьютерных системах».

## Основные аспекты комплексного подхода обеспечения информационно-компьютерной безопасности

Несмотря на совершенствование технологий в области защиты информации, уязвимость автоматизированных систем продолжает возрастать (Рисунок 1). Основная причина сложившейся ситуации состоит в отсутствии комплексного подхода к решению проблемы информационно-компьютерной безопасности. Это приводит не только к ошибкам построения систем защиты, но и к недостаткам в поддержании их актуального состояния.



Рисунок 1 – Причинно-следственная диаграмма текущего состояния проблемы информационно-компьютерной безопасности

Главный принцип комплексного подхода к построению защищённых автоматизированных систем – учёт всех исходных требований, существующих угроз и влияющих на безопасность факторов при комплексном использовании наиболее эффективных мер, методов и средств защиты. Выделяются четыре аспекта рассматриваемого подхода [36]:

* учёт основополагающих требований, вытекающих из нормативных документов, теории и практики защиты информации;
* тщательное и полное выполнение необходимых стадий разработки системы защиты с контролем качества промежуточных и итоговых результатов;
* решение всех базовых задач и подзадач защиты для нейтрализации как явных, так и скрытых угроз;
* обеспечение гарантированности защиты за счёт использования проверенных методов и сертифицированных средств, а также объективной аттестации защищенной автоматизированной системы.

К системам информационно-компьютерной безопасности изначально должны предъявляться следующие основополагающие требования, обеспечивающие максимальную степень защищенности автоматизированных систем:

* соответствие требованиям отечественных нормативных документов (МО, ФСТЭК, ФСБ, гос. стандартов) и международных стандартов (ГОСТ Р ИСО/МЭК 15408 – критерии оценки безопасности информационных технологий, ГОСТ Р ИСО/МЭК 27002 – свод норм и правил менеджмента информационной безопасности и др.);
* многоуровневое построение системы защиты при корректности, полноте и непротиворечивости реализации всех приоритетных функций, без которых невозможно достигнуть требуемой степени защищенности;
* централизованное управление средствами защиты, пользователями, рабочими станциями и ресурсами компьютерной сети на основе правил единой политики безопасности;
* централизованный контроль защищённости и поддержка принятия решений для снижения количества ошибок администрирования и своевременного реагирования на события, связанные с нарушениями информационной безопасности.

Защита информации — это не разовое мероприятие и даже не определённая совокупность проведённых мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационно-компьютерной системы, начиная с самых ранних стадий проектирования, а не только на этапе её эксплуатации. В идеальном случае разработка системы информационно-компьютерной безопасности должна вестись параллельно с разработкой самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счёте, позволит создать более эффективную, как по затратам ресурсов, так и по стойкости систему защиты.

Поэтому высокая степень защищённости автоматизированных систем достигается путем тщательного и полного выполнения необходимых стадий разработки и совершенствования системы защиты с контролем качества промежуточных и итоговых результатов, которые можно свести к этапам анализа, выработки детальных требований и многоуровневого синтеза систем защиты (Рисунок 2).



Рисунок – Базовые этапы построения системы информационно-компьютерной безопасности

При построении систем информационно-компьютерной безопасности часто упрощённо подходят к фазам внедрения системы защиты и её поддержания в актуальном состоянии.

В настоящее время в большинстве случаев установка средств защиты производится на уже реально функционирующие компьютерные системы критических объектов автоматизации. Защищаемая компьютерная система используется для решения важных прикладных задач, часто в непрерывном технологическом цикле, и её пользователи крайне негативно относятся к любому перерыву в её функционировании для установки и настройки средств защиты.

Внедрение системы информационно-компьютерной безопасности осложняется ещё и тем, что правильно настроить средства защиты с первого раза обычно не представляется возможным. Это, как правило, связано с отсутствием детального списка подлежащих защите компьютерных ресурсов, а также непротиворечивого перечня полномочий пользователей по доступу к данным ресурсам. Поэтому, этап внедрения системы информационно-компьютерной безопасности обязательно должен включать действия по первоначальному выявлению, итеративному уточнению и соответствующему изменению настроек средств защиты. Эти же действия неоднократно придётся повторять администратору безопасности и на этапе эксплуатации системы безопасности каждый раз при изменении структуры, технологических схем и условий функционирования компьютерной сети. Если система защиты не обладает достаточной гибкостью и не обеспечивает удобство перенастройки, то она очень быстро становится обузой и обречена на отторжение.

Для поддержки и облегчения действий по внедрению системы информационно-компьютерной безопасности в ней необходимо предусмотреть следующие возможности:

* выборочное подключение имеющихся защитных средств, что обеспечивает поэтапное усиления степени защищенности;
* первоначальную установку отслеживающего режима функционирования средств защиты, при котором несанкционированные действия пользователей фиксируются в системном журнале обычным порядком, но не блокируются (данный режим позволяет выявлять и устранять имеющиеся некорректности в настройках средств защиты без нарушения существующей технологии обработки информации);
* возможности по автоматизированному изменению полномочий пользователей в зависимости от информации, накопленной в системных журналах.

Средства защиты при реализации контрмер должны обеспечивать решение базовых задач защиты для нейтрализации как явных, так и скрытых угроз информационно-компьютерной безопасности:

* защиты компьютерных ресурсов на уровне серверов и рабочих станций локальных вычислительных сетей;
* защиты передаваемой информации и противодействия несанкционированному межсетевому взаимодействию;
* поддержания системы защиты в актуальном состоянии.

Назначение и базовые цели защиты информации в автоматизированных системах представлены ниже (Рисунок 3).

Меры по защите информации, обеспечивающие достижение целей защиты, принимаются путем выполнения соответствующих функций защиты, множество которых должно быть достаточным для обеспечения требуемой степени информационно-компьютерной безопасности в любой момент времени. Множество активных функций определяется текущими условиями хранения и обработки информации в компьютерной системе.



Рисунок – Назначение и базовые цели системы защиты

Любая функция защиты выполняется в соответствии с используемым методом защиты с помощью специально созданных для её выполнения средств. Под методом (способом) защиты понимается алгоритмическое описание процесса решения какой-либо задачи защиты.

Необходимым условием достижения требуемой степени информационно-компьютерной безопасности является принятие всех возможных мер защиты (Рисунок 4):

* морально-этических;
* законодательных;
* организационных;
* технических.

Существующие в стране и специально издаваемые законы и другие нормативно-правовые акты в области информационно-компьютерной безопасности являются законодательным средствами защиты информации. Эти средства составляет пакет Федеральных законов, Указов Президента РФ, постановлений Правительства РФ, а также межведомственных руководящих документов и стандартов. Важнейшими законодательными и нормативными актами РФ являются законы «О государственной тайне», «Об информации, информационных технологиях и о защите информации», «Об электронной подписи», «О персональных данных», «О коммерческой тайне», Гражданский и Уголовный кодексы РФ, а также нормативные документы МО РФ, ФСТЭК и ФСБ России.



Рисунок – Классификация мер, методов и средств комплексной защиты информации