**Лекция 2. Угрозы безопасности программного обеспечения.**

**1. Виды угроз информационной безопасности и классификация источников угроз**

Анализ проблем экономической безопасности необходимо проводить, учитывая взаимосвязи экономических противоречий, угроз и потерь, к которым может приводить реализация угроз. Такой анализ приводит к следующей цепочке:

* источник угрозы (внешняя и/или внутренняя среда предприятия)
* зона риска (сфера экономической деятельности предприятия, способы её реализации, материальные и информационные ресурсы)
* фактор (степень уязвимости данных, информации, программного обеспечения, компьютерных и телекоммуникационных устройств, материальных и финансовых ресурсов, персонала)>
* угроза (вид, величина, направление)
* возможность её реализации (предпосылки, объект, способ действия, скорость и временной интервал действия)
* последствия (материальный ущерб, моральный вред, размер ущерба и вреда, возможность компенсации).

Построение надежной защиты компьютерной системы невозможно без предварительного анализа возможных угроз безопасности системы. Этот анализ должен включать в себя:

• выявление характера хранящейся в системе информации, выделение наиболее опасных угроз (несанкционированное чтение, несанкционированное изменение и т.д.);

• оценку затрат времени и средств на вскрытие системы, допустимых для злоумышленников;

• оценку ценности информации, хранящейся в системе;

• построение модели злоумышленника (другими словами, определение того, от кого нужно защищаться - от постороннего лица, пользователя системы, администратора и т.д.);

• оценку допустимых затрат времени, средств и ресурсов системы на организацию ее защиты.

Основные классы угроз безопасности, направленных против информационных ресурсов:

• угрозы, реализуемые либо воздействием на программное обеспечение и конфигурационную информацию системы, либо посредством некорректного использования системного и прикладного программного обеспечения;

• угрозы, связанные с выходом из строя технических средств системы, приводящим к полному или частичному разрушению информации, хранящейся и обрабатываемой в системе;

• угрозы, обусловленные человеческим фактором и связанные с некорректным использованием сотрудниками программного обеспечения или с воздействием на технические средства, в большей степени зависят от действий и "особенностей" морального поведения сотрудников;

• Угрозы с использованием программных средств*.*

Наиболее многочисленный класс угроз конфиденциальности, целостности и доступности информационных ресурсов связан с получением внутренними и внешними нарушителями логического доступа к информации с использованием возможностей, предоставляемых общесистемным и прикладным программным обеспечением. Большинство рассматриваемых в этом классе угроз реализуется путем локальных или удаленных атак на информационные ресурсы системы внутренними и внешними нарушителями. Результатом осуществления этих угроз становится несанкционированный доступ к данным, управляющей информации, хранящейся на рабочем месте администратора системы, конфигурационной информации технических средств, а также к сведениям, передаваемым по каналам связи.

В этом классе выделяются следующие основные угрозы:

• угрозы техническим средствам

• несанкционированный доступ к приложению;

• внедрение вредоносного программного обеспечения;

• злоупотребление системными ресурсами;

• отказ от подтверждения авторства передаваемой информации;

• сбои системного и сетевого программного обеспечения;

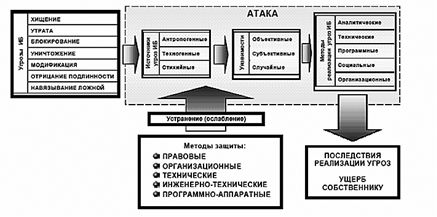
• сбои прикладного программного обеспечения.

Наиболее уязвимы с точки зрения защищенности информационных ресурсов являются так называемые критические компьютерные системы. Под критическими компьютерными системами будем понимать сложные компьютеризированные организационно - технические и технические системы, блокировка или нарушение функционирования которых потенциально приводит к потере устойчивости организационных систем государственного управления и контроля, утрате обороноспособности государства, разрушению системы финансового обращения, дезорганизации систем энергетического и коммуникационно - транспортного обеспечения государства, глобальным экологическим и техногенным катастрофам.

Угрозы можно классифицировать по нескольким критериям:

* по важнейшим составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых направлены угрозы в первую очередь;
* по компонентам информационных систем и технологий (данные, программно-аппаратные комплексы, сети, поддерживающая инфраструктура), на которые угрозы непосредственно нацелены;
* по способу осуществления (случайные или преднамеренные действия, события техногенного или природного масштаба);
* по локализации источника угроз (вне или внутри информационной технологии или системы).

Одна из возможных моделей классификации угроз представлена на рис.1.



**Рис. 1. Модель возможных** угроз системе информационной безопасности и основные классы методов защиты

В ходе анализа необходимо убедиться, что большинство возможных источников угроз и уязвимости идентифицированы и сопоставлены друг с другом, а всем идентифицированным источникам угроз и уязвимостям сопоставлены методы их нейтрализации и устранения.

При выявлении актуальных угроз экспертно-аналитическим методом определяются объекты защиты, подверженные воздействию той или иной угрозы, характерные источники этих угроз и уязвимости, способствующие реализации угроз.

На основании анализа составляется матрица взаимосвязи источников угроз и уязвимостей, из которой определяются возможные последствия реализации угроз (атаки) и вычисляется коэффициент значимости (степени опасности) этих атак как произведение коэффициентов опасности соответствующих угроз и источников угроз, определенных ранее.

Благодаря такому подходу возможно:

* установить приоритеты целей безопасности для субъекта отношений;
* определить перечень актуальных источников угроз;
* определить перечень актуальных уязвимостей;
* оценить взаимосвязь уязвимостей, источников угроз, возможности их осуществления;
* определить перечень возможных атак на объект;
* разработать сценарии возможных атак;
* описать возможные последствия реализации угроз;
* разработать комплекс защитных мер и систему управления экономической и информационной безопасностью предприятия.

Пользователи могут быть источниками следующих угроз:

* намеренная (встраивание логической бомбы, которая со временем разрушит программное ядро или приложения) или непреднамеренная потеря или искажение данных и информации, "взлом" системы администрирования, кража данных и паролей, передача их посторонним лицам и т.д.;
* нежелание пользователя работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности или при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками) и намеренный вывод из строя её программно-аппаратных устройств;
* невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т. п.).

Эффективный способ борьбы с непреднамеренными ошибками — максимальная автоматизация и стандартизация, информационных процессов, использование устройств "защита от дурака" (Fool Proof Device), регламентация и строгий контроль действий пользователей. Необходимо также следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Основными источниками внутренних системных отказов являются:

* невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т. п.);
* отступление (случайное или умышленное) от установленных правил эксплуатации;
* выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т. п.);
* ошибки конфигурирования системы;
* отказы программного и аппаратного обеспечения;
* разрушение данных;
* разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

* нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
* разрушение или повреждение помещений;
* невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т. п.).

2. **Несанкционированное копирование, распространение и использование программ**

Для предотвращения незаконных действий с программным обеспечением возможны следующие сценарии поведения для зарегистрированных пользователей:

* периодическое получение новых версий программного продукта, соответствующей документации, специальных журналов;
* возможность получения оперативной консультации;
* проведение семинаров и курсов по обучению использованию программного продукта;
* предоставление скидки при покупке следующей версии продукта.

3. **Разрушающие программные средства (РПС)**

Угрозы безопасности информации и программного обеспечения КС возникают как в процессе их эксплуатации, так и при создании этих систем, что особенно характерно для процесса разработки ПО, баз данных и других информационных компонентов КС.

Наиболее уязвимы с точки зрения защищенности информационных ресурсов являются так называемые критические компьютерные системы. Под критическими компьютерными системами будем понимать сложные компьютеризированные организационно-технические и технические системы, блокировка или нарушение функционирования которых потенциально приводит к потере устойчивости организационных систем государственного управления и контроля, утрате обороноспособности государства, разрушению системы финансового обращения, дезорганизации систем энергетического и коммуникационно транспортного обеспечения государства, глобальным экологическим и техногенным катастрофам.

Под компьютерным вирусом следует понимать программы, способные размножаться, прикрепляться к другим программам, передаваться по телекоммуникационным каналам.

Под алгоритмической закладкой будем понимать преднамеренное завуалированное искажение какой-либо части алгоритма решения задачи, либо построение его таким образом, что в результате конечной программной реализации этого алгоритма в составе программного компонента или комплекса программ, последние будут иметь ограничения на выполнение требуемых функций, заданных спецификацией, или вовсе их не выполнять при определенных условиях протекания вычислительного процесса, задаваемого семантикой перерабатываемых программой данных.

Под программной закладкой будем понимать совокупность операторов и (или) операндов, преднамеренно в завуалированной форме включаемую в состав выполняемого кода программного компонента на любом этапе его разработки. Программная закладка реализует определенный несанкционированный алгоритм с целью ограничения или блокирования выполнения программным компонентом требуемых функций при определенных условиях протекания вычислительного процесса, задаваемого семантикой перерабатываемых программным компонентом данных, либо с целью снабжения программного компонента не предусмотренными спецификацией функциями, которые могут быть выполнены при строго определенных условиях протекания вычислительного процесса.

Действия алгоритмических и программных закладок условно можно разделить на три класса: изменение функционирования вычислительной системы (сети), несанкционированное считывание информации и несанкционированная модификация информации, вплоть до ее уничтожения.

В первом классе воздействий выделим следующие:

* уменьшение скорости работы вычислительной системы (сети);
* частичное или полное блокирование работы системы (сети);
* имитация физических (аппаратурных) сбоев работы вычислительных средств и периферийных устройств;
* переадресация сообщений;
* обход программно-аппаратных средств криптографического преобразования информации;
* обеспечение доступа в систему с непредусмотренных периферийных устройств.

Несанкционированное считывание информации, осуществляемое в автоматизированных системах, направлено на:

* считывание паролей и их отождествление с конкретными пользователями;
* получение секретной информации;
* идентификацию информации, запрашиваемой пользователями;
* подмену паролей с целью доступа к информации;
* контроль активности абонентов сети для получения косвеннои информации о взаимодействии пользователей и характере информации, которой обмениваются абоненты сети.

Несанкционированная модификация информации является наиболее опасной разновидностью воздействий программных закладок, поскольку приводит к наиболее опасным последствиям. В этом классе воздействий можно выделить следующие:

* разрушение данных и кодов исполняемых программ внесение тонких, трудно обнаруживаемых изменений в информационные массивы;
* внедрение программных закладок в другие программы и подпрограммы (вирусный механизм воздействий);
* искажение или уничтожение собственной информации сервера и тем самым нарушение работы сети;
* модификация пакетов сообщений.

С точки зрения времени внесения программных закладок в программы их можно разделить на две категории: априорные и апостериорные, то есть закладки, внесенные при разработке ПО (или «врожденные») и закладки, внесенные при испытаниях, эксплуатации или модернизации ПО (или «приобретенные») соответственно.

Таким образом, рассмотренные программные средства деструктивного воздействия по своей природе носят, как правило, разрушительный, вредоносный характер, а последствия их активизации и применения могут привести к значительному или даже непоправимому ущербу в тех областях человеческой деятельности, где применение компьютерных систем является жизненно необходимым. В связи с этим такие вредоносные программы будем называть разрушающими программными средствами (РПС), а их обобщенная классификация может выглядеть следующим образом:

* компьютерные вирусы - программы, способные размножаться, прикрепляться к другим программам, передаваться по линиям связи и сетям передачи данных, проникать в электронные телефонные станции и системы управления и выводить их из строя;
* программные закладки программные компоненты, заранее внедряемые в компьютерные системы, которые по сигналу или в установленное время приводятся в действие, уничтожая или искажая информацию, или дезорганизуя работу программнотехнических средств;
* способы и средства, позволяющие внедрять компьютерные вирусы и программные закладки в компьютерные системы и управлять ими на расстоянии.

**4. Принципы обеспечения безопасности программного обеспечения**

Один из возможных подходов к созданию модели технологической безопасности ПО может основываться на обобщенной концепции технологической безопасности компьютерной инфосферы, которая определяет методологический базис, направленный на решение, в том числе, следующих основных задач:

• создания теоретических основ для практического решения проблемы технологической безопасности ПО;

• создания безопасных информационных технологий;

• развертывания системы контроля технологической безопасности компьютерной инфосферы.

Модель угроз должна включать:

* полный реестр типов возможных программных закладок;
* описание наиболее технологически уязвимых мест компьютерных систем (с точки зрения важности и наличия условий для скрытого внедрения программных закладок);
* описание мест и технологические карты разработки программных средств, а также критических этапов, при которых наиболее вероятно скрытое внедрение программных закладок;
* реконструкцию замысла структур, имеющих своей целью внедрение в ПО заданного типа (класса, вида) программных закладок диверсионного типа;
* психологическии портрет потенциального диверсанта в компьютерных системах.

**Основные принципы обеспечения безопасности ПО.**

В качестве объекта обеспечения технологической и эксплуатационной безопасности ПО рассматривается вся совокупность его компонентов в рамках конкретной. В качестве доминирующей должна использоваться стратегия сквозного тотального контроля технологического и эксплуатационного этапов жизненного цикла компонентов ПО. Совокупность мероприятий по обеспечению технологической и эксплуатационной безопасности компонентов ПО должна носить, по возможности, конфиденциальный характер. Необходимо обеспечить постоянный, комплексный и действенный контроль за деятельностью разработчиков и пользователей компонентов ПО. Кроме общих принципов, обычно необходимо конкретизировать принципы обеспечения безопасности ПО на каждом этапе его жизненного цикла. Далее приводятся один из вариантов разработки таких принципов.

***Принципы обеспечения технологической безопасности при обосновании, планировании работ и проектном анализе ПО*.**

Принципы обеспечения безопасности ПО на данном этапе включают следующие принципы:

*Комплексности обеспечения безопасности* ПО, предполагающей рассмотрение проблемы безопасности информационно-вычислительных процессов с учетом всех структур КС, возможных каналов утечки информации и несанкционированного доступа к ней, времени и условий их возникновения, комплексного применения организационных и технических мероприятий.

*Планируемости применения средств безопасности программ*, предполагающей перенос акцента на совместное системное проектирование ПО и средств его безопасности, планирование их использования в предполагаемых условиях эксплуатации.

*Обоснованности средств обеспечения безопасности* ПО, заключающейся в глубоком научно-обоснованном подходе к принятию проектных решений по оценке степени безопасности, прогнозированию угроз безопасности, всесторонней априорной оценке показателей средств защиты.

*Достаточности защищенности программ*, отражающей необходимость поиска наиболее эффективных и надежных мер безопасности при одновременной минимизации их стоимости.

*Гибкости управления защитой программ*, требующей от системы контроля и управления обеспечением безопасности ПО способности к диагностированию, опережающей нейтрализации, оперативному и эффективному устранению возникающих угроз.

*Заблаговременности разработки средств обеспечения безопасности и контроля производства* ПО, заключающейся в предупредительном характере мер обеспечения технологической безопасности работ в интересах недопущения снижения эффективности системы безопасности процесса создания ПО.

*Документируемости технологии создания программ*, подразумевающей разработку пакета нормативно-технических документов по контролю программных средств на наличие преднамеренных дефектов.

***Принципы достижения технологической безопасности ПО в процессе его разработки***

Принципы обеспечения безопасности ПО на данном этапе включают следующие принципы:

*Регламентации технологических этапов разработки* ПО, включающей упорядоченные фазы промежуточного контроля, спецификацию программных модулей и стандартизацию функций и формата представления данных.

*Автоматизации средств контроля управляющих и вычислительных программ* на наличие преднамеренных дефектов.

*Создания типовой общей информационной базы алгоритмов, исходных текстов и программных средств,* позволяющих выявлять преднамеренные программные дефекты.

*Последовательной многоуровневой фильтрации программных модулей* в процессе их создания с применением функционального дублирования разработок и поэтапного контроля.

*Типизации алгоритмов, программ и средств информационной безопасности*, обеспечивающей информационную, технологическую и программную совместимость, на основе максимальной их унификации по всем компонентам и интерфейсам.

*Централизованного управления базами данных проектов* ПО *и администрирование технологии их разработки* с жестким разграничением функций, ограничением доступа в соответствии со средствами диагностики, контроля и защиты.

*Блокирования несанкционированного доступа* соисполнителей и абонентов государственных и негосударственных сетей связи, подключенных к стендам для разработки программ.

*Статистического учета и ведения системных журналов* о всех процессах разработки ПО с целью контроля технологической безопасности. Использования только сертифицированных и выбранных в качестве единых инструментальных средств разработки программ для новых технологий обработки информации и перспективных архитектур вычислительных систем. программа компьютер вирус информационный безопасность

***Принципы обеспечения технологической безопасности на этапах стендовых и приемосдаточных испытаний***

Принципы обеспечения безопасности ПО на данном этапе включают принципы:

*Тестирования* ПО на основе разработки комплексов тестов, параметризуемых на конкретные классы программ с возможностью функционального и статистического контроля в широком диапазоне изменения входных и выходных данных.

*Проведения натурных испытаний программ* при экстремальных нагрузках с имитацией воздействия активных дефектов.

*Осуществления «фильтрации»* программных комплексов с целью выявления возможных преднамеренных дефектов определенного назначения на базе создания моделей угроз и соответствующих сканирующих программных средств. Разработки и экспериментальной отработки средств верификации программных изделий.

*Проведения стендовых испытаний* ПО для определения непреднамеренных программных ошибок проектирования и ошибок разработчика, приводящих к невыполнению целевых функций программ, а также выявление потенциально «узких» мест в программных средствах для разрушительного воздействия. Отработки средств защиты от несанкционированного воздействия нарушителей на ПО.

*Сертификации программных изделий по требованиям безопасности* с выпуском сертификата соответствия этого изделия требованиям технического задания.

***Принципы обеспечения безопасности при эксплуатации программного обеспечения*** Принципы обеспечения безопасности ПО на данном этапе включают принципы:

*Сохранения эталонов и ограничения доступа к ним* программных средств, недопущение внесения изменений в эталоны. Профилактического выборочного тестирования и полного сканирования программных средств на наличие преднамеренных дефектов.

*Идентификации* ПО на момент ввода его в эксплуатацию в соответствии с предполагаемыми угрозами безопасности ПО и его контроль.

*Обеспечения модификации программных изделий* во время их эксплуатации путем замены отдельных модулей без изменения общей структуры и связей с другими модулями.

*Строгого учета и каталогизации* всех сопровождаемых программных средств, а также собираемой, обрабатываемой и хранимой информации.

*Статистического анализа информации* обо всех процессах, рабочих операциях, отступлениях от режимов штатного функционирования ПО.

*Гибкого применения дополнительных средств защиты* ПО в случае выявления новых, непрогнозируемых угроз информационной безопасности.

.