МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.Ю. Щеглов, К.А. Щеглов

МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ФОРМАЛЬНОГО ПРОЕКТИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебное пособие

Санкт-Петербург

2015

Щеглов А.Ю., Щеглов К.А.Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие.– СПб: Университет ИТМО, 2015. – 93с.

В учебном пособии приводится математический аппарат, который может использоваться для формального проектирования систем защиты информационных систем, реализуемого с целью определения требований к оптимальному набору решаемых задач защиты и расчета значений параметров и характеристик безопасности проектируемой системы защиты. Рассматриваются методы моделирования характеристик безопасности и математические модели угрозы уязвимости, угрозы атаки, угрозы безопасности информационной системы в целом, математическая модель потенциального нарушителя безопасности, основанные на использовании в качестве элемента информационной безопасности угрозы уязвимости. Представлены интерпретации угрозы атаки и угрозы безопасности информационной системы соответствующими схемами резервирования, позволяющие определить критерии оптимальности системы защиты, используемые при ее проектировании. Исследованы вопросы резервирования элементов информационных систем в области информационной безопасности, показаны фундаментальные противоречия задач и методов резервирования, используемых для повышения уровня надежности и безопасности информационной системы, пути их решения. Материал пособия разбит на 3 раздела, введение и заключение.
Пособие может быть использовано при подготовке магистров по направлениям 09.04.04 «ПРОГРАММНАЯ ИНЖЕНЕРИЯ», 09.04.01 “ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА”, а также инженеров и аспирантов.

Рекомендовано к печати ученым советом факультета Компьютерных технологий и управления, протокол 21 апреля 2014 г., протокол № 4.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Любое проектирование, в том числе проектирование системы защиты информации информационной системы, основано на реализации соответствующей процедуры оптимизации, в противном случае нет проектирования, невозможного без использования соответствующих критериев оптимальности. В этом случае можно лишь говорить о каком-либо построении системы защиты, термин "проектирование" здесь уже неуместен. К сожалению, во многом именно ввиду отсутствия подобных обоснованных критериев, которые, естественно, должны оцениваться количественно, на сегодняшний день на практике реализуется не проектирование, а построение систем защиты информационных систем[2,3].Оно заключаетсяв реализации защиты от потенциально возможных угроз атак на информационную систему, отнесенных каким-либо образом, как правило, на основе каких-либо субъективных (так называемых экспертных) оценок к актуальным для защищаемой информационной системы, применительно к которой создается система защиты. При этом, при так называемом проектировании, опять же, исходя из каких-либо соображений (не имея количественных оценок), требуется не только отнести угрозу к актуальной для конкретной информационной системы, для которой проектируется система защиты, но и необходимо учесть возможность и сложность реализации атаки, а также желание и возможность ее реализации потенциальным нарушителем безопасности, для чего строится модель нарушителя.Опять же используются экспертные оценки.

Нельзя забывать и еще об одном важном аспекте проектирования, в нашем случае – системы защиты. При проектировании системы защитынеобходимо определить то, какие задачи должны решаться системой защиты, необходимо сформулировать требования к параметрам и к характеристикам создаваемой системы защиты, для чего, опять же, необходимо моделирование с целью получения соответствующих количественных оценок. Все это можно отнести к задачам формального проектирования системы защиты. Отметим, что решение задачи формального проектирования системы защиты информационной системы не дает ответа на вопрос, как строить систему защиты. Эти вопросы излагаются в учебном пособии [28]. Задачей формального проектирования системы защиты информационной системы является определение требований к набору (естественно, что это оптимизационная задача) решаемых ею задач и требований к эксплуатационным параметрам и характеристикам безопасности системы защиты.

Естественно, что, не имея возможности получения каких-либо обоснованных количественных оценок, не только о каких-либо оптимальных решениях говорить не приходится, но, что гораздо хуже, трудно оценить (а количественно – просто невозможно,

поскольку отсутствуют количественные критерии) эффективность построенной системы защиты.

Отличительной особенностью излагаемого в учебном пособии математического аппарата является использование в качестве элемента информационной безопасности не угрозы атаки, а угрозы уязвимости. Уязвимость может быть охарактеризована стохастическими свойствами: с какой-то интенсивностью выявляется (возникает) и устраняется в информационной системе. Именно угрозы уязвимостей в конечном счете и создают угрозу атаки, которая может быть реализована нарушителем. Поскольку возникновение и устранение уязвимостейс определенными оговорками может интерпретироваться как возникновение и устранение отказа (в данном случае характеристики безопасности информационной системы), можно предположить, что для решения рассматриваемых задач моделирования – моделирования отказов и восстановлений характеристики безопасности – может быть использован математический аппарат теории надежности. Однако в теории надежности задача моделирования собственно в своей постановке принципиально отличается. Там нет понятия нарушителя безопасности, осуществляющего целенаправленное воздействие на систему, нет различия целей подобного воздействия: нарушение конфиденциальности, целостности и доступности обрабатываемой информации и т.д. Таким образом, исходя из того, что и в теории надежности, и в теории информационной безопасности существуют в чем-то схожие понятия отказов и восстановлений соответствующих характеристик, потенциально математический аппарат теории надежности может быть использован в теории информационной безопасности для рассматриваемых задач моделирования, но, естественно, с существенной адаптацией под особенности решаемых здесь задач.

Все эти вопросы исследуются в данном учебном пособии, включая изложение математического аппарата, основанного на использовании марковских процессов, который может использоваться для формального проектирования систем защиты информационных систем, реализуемого с целью определения оптимального набора задач защиты и расчета значений параметров и характеристик безопасности проектируемой системы защиты.

1. МАТЕМАТИЧЕСКИЕМОДЕЛИБЕЗОПАСНОСТИ

1.1. Общие положения

Под угрозой информационной безопасности понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации; под уязвимостью, являющейся источником угрозы, – свойство информационной системы, обусловливающее возникновение угрозы безопасности обрабатываемой в ней информации, под атакой – попытка преодоления системы защиты информационной системы[1], т.е. попытка реализации угрозы, создаваемой уязвимостью.Естественно, что атака предполагает использование (эксплуатацию) уязвимостей.

С учетом того, что под безопасностью информации понимается [1] состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность, имеет смысл соответствующим образом классифицировать угрозы: угроза конфиденциальности информации, угроза целостности и доступности информации; и атаки: по реализуемым целям осуществления несанкционированного доступа.

Замечание. В общем случае для угроз может быть введена более детальная классификация, получаемая на основе классификации условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации, например, угроза конфиденциальности информации, возникающая при подключении компьютера к внешней сети.

Под несанкционированным доступом [1] понимается доступ к информации или к ресурсам информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа. Т.е. несанкционированный доступ – это результат атаки, реализуемой с некоторой целью, соответственно, с целью раскрытия конфиденциальности информации, нарушения ее целостности или доступности.

Большинство известных подходов к моделированию, отличающихся тем, какие параметры при моделировании ими используются в качестве входной информации и какие характеристики моделируемой системы рассчитываются и поступают на выход модели (строятся модели с использованием теории вероятностей, случайных процессов, сетей Петри, теории автоматов, теории графов, нечетких множеств, теории катастроф, энтропийного подхода и др.), предполагает использование в качестве простейшего элемента безопасности угрозу атакина информационную систему [4, 8-10,12, 15, 18].

С использованием в качестве простейшего элемента безопасности угрозы атаки связан ряд принципиальных недостатков. Практическая применимость подобных моделей крайне осложняется ввидунеобходимости экспертного задания ключевой характеристики безопасности – вероятности возникновения угрозы атаки. При моделировании, основанном на использовании

в качестве простейшего элемента безопасности угрозы атаки, возникновение различных угроз атак рассматривается в качестве независимых событий, исходя из чего используются соответствующие расчетные формулы. Однако подобный исходный посыл некорректен, т.к. реальные угрозы атак создаются выявляемыми в системе уязвимостями, при этом событиявозникновения угроз атак, как правило, зависимы по уязвимостям, поскольку многимиатаками эксплуатируются одни и те же уязвимости. Например, подавляющая часть угроз атак предполагает внедрение и последующее исполнение на защищаемом компьютере вредоносной программы: используется уязвимость системы, позволяющая исполнять создаваемые в процессе работы интерактивными пользователями файлы [24]. Все эти угрозы атак зависимы по данной уязвимости, рассмотрение их возникновения как независимых событий не позволяет построить корректную математическую модель (это будет обосновано далее). Важным является и то, что оперируя при моделировании не простейшим элементом безопасности, каким является уязвимость (соответственно угроза уязвимости), аугрозой атаки, невозможно обосновать требования к входным параметрам построенной модели. На практике по причине простоты построения соответствующих моделей, как правило, используются марковские процессы (потоки без последействия). Но возникает вопрос: насколько это корректно применительно к разнородным угрозам атак (а это уже вопрос адекватности получаемых моделей), какие условия ими моделируются, как следствие, как интерпретировать полученные результаты?При проектировании же системы защиты информационной системы важно то, чтов конечном счете системой защиты, если ее рассматривать не как некую абстракцию, а попытаться реально спроектировать и построить, защита от угроз атак реализуется нивелированием именно соответствующих уязвимостей, создающих эти угрозы атак. При этом, поскольку, как правило, угроза атаки создается некоторой совокупностью угроз уязвимостей, существуют альтернативные варианты решения задачи защиты, как следствие, можно говорить об оптимизационной задаче при проектировании системы защиты информации.

С учетом сказанногоможно сделать вывод о том, что в качестве простейшего элемента безопасности информационной системы следует рассматривать уязвимость (угрозу уязвимости), что логично, т.к. в конечном счете угроза атаки создается выявляемыми в системе уязвимостями.

С точки зрения проектирования системы защиты информационной системы к исследуемым угрозам уязвимостей, характеризующим соответствующее свойство информационной системы, должны быть отнесенытехнологические недостатки построения информационной системы, включая отсутствие в системе необходимых функций защиты, а также ошибки в используемом прикладном и системном программном обеспечении, включая

систему защиты, позволяющие осуществить обход реализованных функций защиты (реализовать атаку).

Замечание. Поскольку нас интересуют вопросы проектирования системы защиты, не будем рассматривать угрозы, которые могут использоваться при реализации атаки, не связанныес функциональными и с эксплуатационными характеристиками систем защиты, например, ошибки администрирования, в том числе настройки системы защиты информационной системы.

1.2. Угроза уязвимости как простейший элемент безопасности информационной системы. Модели угрозы уязвимости

Под потенциальной угрозой уязвимости для информационной системы понимаем угрозу, возникновение которой потенциально возможно в системе, под реальной же – реально возникшую угрозу (угроза присутствует в системе, соответствующая уязвимость выявлена и не устранена).Угроза атаки, которая также может быть охарактеризована как потенциальная и реальная,как правило, создается соответствующей совокупностью угроз уязвимостей. Например, угроза атаки на повышение привилегий создается следующей совокупностью угроз уязвимостей[26]: возможность несанкционированной установки на компьютер интерактивным пользователем (под его учетной записью без ведома пользователя) вредоносной программы, в том числе из внешней сети (технологическая уязвимость), выявление в программномсистемном средстве, запускаемом с системными правами, ошибки программирования, возможность исполнения созданного интерактивным пользователем в процессе работы файла (технологическая уязвимость), невозможность задания разграничений прав доступа к файловым объектам для процессов, запускаемых с системными правами (технологическая уязвимость), далее в зависимости от цели атаки. Атака при этом состоит во внедрении нарушителем вредоносной программы, ее запуск с системными правами, реализация несанкционированного доступа с какой-либо целью к файловым объектам, используемым в системе для хранения конфиденциальных данных, в обход разграничительной политики доступа, реализуемой системой защиты для интерактивных пользователей. На этом же примере можем проиллюстрировать и реализацию системы защиты применительно к нивелированию отдельных угроз уязвимостей. Системой защиты может предотвращаться возможность установки на компьютер исполняемых файлов [11], может предотвращаться возможность исполнения созданных интерактивными пользователями файлов, в том числе и с системными правами [24], может быть реализована разграничительная политика доступа к файловым объектам для процессов, запускаемых с системными правами [27]. Как видим, задача нивелирования угрозы атаки при реализации системы защиты в любом случае сводится к задаче нивелирования какой-либо угрозы уязвимости. Следовательно, при проектировании системы

защиты необходима оценка актуальности для нивелирования ее системой защиты именно угрозы уязвимости, естественно, применительно к актуальной угрозе атаки.

Акцентируем внимание на следующем важном моменте, который должен быть учтен при последующем моделировании. Здесь и далее, говоря об уязвимости и об угрозе уязвимости, в общем случае мы понимаем некую совокупность однотипныхуязвимостей, создающих одни и те же условия для реализации атаки на информационную систему. Например, выявляемые ошибки в системных программных средствах, позволяющие запустить программу с системными правами, мы рассматриваем как одну уязвимость.Вместе с тем для реализации атаки на повышение привилегий могут использоваться выявленные уязвимости (ошибки программирования) в различных компонентах системы, работающих в режиме ядра, например,для ОС семейства Windows– это драйвер подсистемы Windows (Win32k.sys), системные драйверы (KM drives) и ядро ntoskrnl (NTOS)[25,29].

С точки зрения последующего моделирования важным является необходимость учета того, что в общем случае в системе одновременно может присутствовать несколько выявленных и не устраненных однотипных уязвимостей– реальных угроз уязвимости.

В отношении выявляемых и исправляемых уязвимостей постоянно ведется соответствующая статистикаи аналитическая обработка с целью предоставления пользователям оперативной информации о выявленных уязвимостях и об уровне их критичности. На сегодняшний день наиболее широкое практическое использование нашли следующие способы классификации и количественной оценки актуальности уязвимостей: схема классификации уязвимостей NIPC, шкала анализа уязвимостей SANS, система оценки критичности уязвимостей Microsoft, система оценки уязвимостей по стандарту PCI DSS, системы US—CERT, CVSS и nCircle[31, 34-37, 39]. Они различаются учитываемыми при классификации уязвимостей параметрами и шкалами оценки уязвимостей.

В качестве примера рассмотрим Общую Систему Оценки Уязвимости (CommonVulnerabilityScoringSystem, CVSS). Данная система предназначена для классификации уязвимостей по шкале критичности от 0 до 10:

- 0,0 – 3,9 — низкая степень;
- 4,0 – 6,9 — средняя степень;
- 7,0 – 9,9 — высокая степень;
- 10 — критическая степень.

Оценка (отнесение к уровню критичности) уязвимости производится на основе набора показателей: вектор доступа, сложность доступа, аутентификация, влияние на конфиденциальность, влияние на целостность, влияние на доступность.

Вектор доступа (AccessVector) определяет, как уязвимость может быть обнаружена и использована.

- Local – злоумышленнику необходим физический доступ к компьютеру;
- Adjacent Network – злоумышленнику необходим доступ к локальной сети;
- Network – уязвимость может быть использована из сети Интернет.

Сложность доступа (AccessComplexity) определяет, насколько сложно провести атаку на систему через уязвимость после получения доступа к ней.

- High – злоумышленнику необходимо иметь высокую квалификацию, использовать нестандартные пути реализации атаки и обладать значительной информацией о системе. Конфигурация ПО является достаточно экзотической;
- Medium – злоумышленник должен иметь ограниченные права в системе. Конфигурация ПО отличается от конфигурации по умолчанию;
- Low – конфигурация по умолчанию. Круг тех, кто может являться злоумышленником, не ограничен.

Аутентификация (Authentification) определяет, сколько уровней аутентификации и авторизации должен пройти злоумышленник, прежде чем он получит возможность использовать уязвимость в системе.

- Multiple – множественная аутентификация и авторизация;
- Single – однократная авторизация;
- None – отсутствие аутентификации и авторизации.

Влияние на конфиденциальность (ConfidentialityImpact) определяет влияние успешной атаки с использованием уязвимости на конфиденциальность системы и данных.

- None – отсутствие влияния;
- Partial – злоумышленник получает доступ к ограниченному набору данных;
- Complete – злоумышленник получает полный доступ ко всем данным.

Влияние на целостность (IntegrityImpact) определяет влияние успешной атаки с использованием уязвимости на целостность данных и системы.

- None – отсутствие влияния;
- Partial – частичная потеря целостности (возможна модификация части конфигурации системы, часть данных может быть подменена и пр.);
- Complete – возможна подмена любых данных, модификация конфигурации и процессов всей системы.

Влияние на доступность (AvailabilityImpact) определяет влияние успешной атаки с использованием уязвимости на доступность системы.

- None – отсутствие влияния;
- Partial – частичная недоступность (падение производительности системы или ее частей, непродолжительные перерывы в доступности данных);
- Complete – полная недоступность системы, отказ в обслуживании.

Из представленного примера видим, что классификация уязвимостей (отнесение их к уровню критичности) основана на использовании экспертных оценок. Кроме того, можем сделать вывод и о том, что статистика по выявляемым и устраняемым уязвимостям непрерывно ведется, известна, доступна, их стохастические параметры (об этом далее) могут быть определены, что позволяет проводить в отношении угроз уязвимостей соответствующий вероятностный анализ.

Таким образом, оценка актуальности уязвимости, определяемая мерой критичности уязвимости, формируемая известными подходами к оцениванию, исходя из сложности ее выявления, использования и целей эксплуатации злоумышленником, позволяет делать выводы о необходимости и экстренности принятия каких-либо мер в отношении выявленной уязвимости, в том числе каких-либо организационных мер, но при этом никоим образом не затрагивает стохастических свойств обнаружения и устранения уязвимостей, что не позволяет осуществлять каких-либо прогнозов в отношении последующего выявлениях каких-либо видов уязвимостей, позволяющих осуществлять атаки соответствующих типов, в процессе функционирования системы.

Пример отчета по количеству выявленных уязвимостей за год с отнесением их к уровню критичности, наглядно иллюстрирующего современное положение дел в информационной безопасности, приведен на рис.1[30].

Отметим, что в соответствии с используемой классификацией уровня критичности уязвимости на уровень безопасности информационной системы существенно влияют уязвимости, характеризуемые критической, высокой и средней степенями опасности (например, следуя классификации уязвимостей [30], к уязвимостям средней степени опасности относятся уязвимости, которые позволяют удаленный отказ в обслуживании, неавторизованный доступ к данным или выполнение произвольного кода), см. рис.1.

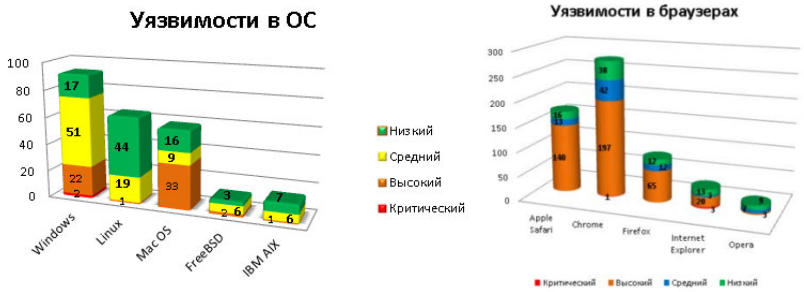


Рис.1. Статистика обнаруженных уязвимостей в ОС и в браузерах за 2011 г.

Информации в открытых источниках о выявляемых и устраняемых уязвимостях достаточно. Используя данную статистику, можно определить соответствующие стохастические параметры угрозы уязвимости: интенсивность возникновения (выявления)λ и интенсивность устранения μ , и построить соответствующую математическую модель, позволяющую определять вероятность готовности информационной системы к безопасной эксплуатации в отношении угрозы уязвимости $P_{0y} = f(\lambda, \mu)$[21]. Данная характеристика угрозы уязвимости может позиционироваться в качестве количественной оценки ее актуальности.

Замечание. Уязвимости по своей сути разнородны. Некоторые из них при выявлении не создают реальной угрозы до тех пор, пока нарушителем не предпринято соответствующих действий, позволяющих реализовать реальную угрозу, например, не создано программного средства, позволяющего осуществить атаку на выявленную уязвимость (эксплойта). Сложность использования уязвимостей соответствующего типа можно учесть, определяя параметрλ только для той части уязвимостей, которые реально эксплуатировались –для которых были разработаны и использовалисьэксплойты (такая статистика так же ведется). Например, в 2013 году, несмотря на множество выявленных, эксплуатировались лишь несколько уязвимостей драйвера Win32k.sys[29].

В отношении угрозы уязвимости информационная система в определенном смысле может рассматриваться как система с отказами и восстановлениями характеристики безопасности. Отказом здесь выступает выявление уязвимости, а восстановлением –устранение выявленной уязвимости.

В теории надежности для моделирования систем с отказами и восстановлениями (в данном случае – ремонта) объектов – характеристики надежности, как правило, используется аппарат марковских случайных процессов при допущениях о пуассоновском характере потока заявок и о показательном распределении времени обслуживания[14]. Как известно, процесс, протекающий в физической системе, называется марковским (или процессом без последействия), если для каждого момента времени вероятность любого состояния системы в будущем зависит только от состояния системы в настоящий момент времени и не зависит от того, каким образом система пришла в это состояние. Рассмотрим, может ли использоваться (корректно ли использование, а если корректно, то как могут интерпретироваться получаемые при моделированиирезультаты) данный математический аппарат в нашем случае – для моделирования систем с отказами и восстановлениями, но уже характеристики безопасности.

С этой целью проанализируем, что собою представляют уязвимости, выявление которых в системе создает реальную угрозу атак. Как отмечали, возникновение уязвимости в информационной системе может быть вызвано двумя причинами: отсутствие, либо

некорректность решения соответствующей задачи защиты, либо ошибки реализации средств информационной системы, например, ошибки программирования, которые могут эксплуатироваться нарушителем для обхода защиты. В качестве параметров угрозы уязвимости рассматриваем интенсивность возникновения уязвимости λ и интенсивность устранения уязвимостиμ. Под возникновением уязвимости (здесь и далее) естественно понимаем ее выявление нарушителем безопасности.

С одной стороны, предполагая, что система содержит конечное (пусть и очень большое) количество не выявленных уязвимостей, можем заключить, что в данном случае процесс не является марковским, поскольку выявление и устранение каждой уязвимости приводит к изменению их числа на конечном исходном множестве, т.е. имеем процесс с последействием. При этом входной поток не будет являться пуассоновским, поскольку в этих предположениях $\lambda \neq const$. Однако оценим, как будут изменяться параметры уязвимости в процессе эксплуатации информационной системы. Очевидно, что в общем случае интенсивность возникновения уязвимостиλ попрошествии некоторого времени будет снижаться, поскольку в первую очередь нарушителем будут выявляться наиболее простые недочеты функциональной реализации защиты и ошибки в программном обеспечении (увеличение сложности выявления уязвимости естественно приведет к снижению интенсивности λ). В отношении же параметра μможем сказать, что он никак не связан со сложностью выявления уязвимости нарушителем безопасности, определяется исключительно типом уязвимости (например, ошибки в системных драйверах и в приложениях требуют различной трудоемкости исправления), т.е. для каждого типа уязвимости можем принять: $\mu = const$.

Теперь допустим, что мы спроектировали систему защиты, применив формальную экстраполяцию (прогнозная экстраполяция здесь мало применима ввиду высокой интенсивности переходов на новые версии программных средств в современных информационных системах) с использованием марковской модели. Тем самым при моделировании мы предположили, что поток без последействия, т.е. интенсивности возникновения уязвимости λ и устранения уязвимости μ будут неизменными в процессе последующей эксплуатации защищенной информационной системы. Очевидно, что с учетом сказанного ранее (а именно, что значение λ будет только уменьшаться, а μостанется неизменным в процессе последующей эксплуатации системы), используя подобную модель, мы найдем граничные (при худших для системы условиях) значения требуемых характеристик, учет которых гарантирует, что "хуже не будет". На самом же деле, определения значений именно таких характеристик при проектировании системы защиты в предположении невозможности корректного прогнозирования изменения их значений во временине требуется (не можем же мы проектировать систему защиты, оперируя заниженными значениями

параметров уязвимости). Вот если бы последействие приводило к увеличению λ в процессе эксплуатации информационной системы, тогда другое дело, подобное последействие при моделировании необходимо было бы в обязательном порядке учитывать (далее проиллюстрируем сказанное на примере оценки эффективности антивирусных средств защиты).

Из сказанного можем сделать крайне важный вывод о том, что при моделировании характеристик угрозы безопасности информационной системы могут использоваться марковские модели, которые позволяют в данном случае определять граничные значения характеристик безопасности, которые и должны использоваться при проектировании системы защиты в предположении невозможности построения корректного прогноза в отношении изменения значений параметров угроз уязвимостей во времени.

С учетом того, что вероятностью одномоментного появления в системе нескольких однотипных уязвимостей (не одновременного присутствия, именно возникновения реальных угроз уязвимостей) можем пренебречь, процесс возникновения и устранения в системе угрозы уязвимости может быть описан схемой "гибели и размножения"[6,16]. Тогда для случая одного обслуживающего прибора искомая характеристика безопасности – стационарный коэффициент готовности (в данном случае готовности к безопасной эксплуатации в отношении угрозы уязвимости)определяется следующим образом:

$$P_{0y} = 1 - \rho,$$

где

$$\rho = \lambda/\mu,$$

а вероятность наличия в системе одновременно *R*не устраненных уязвимостей (реальных угроз уязвимостей):

$$P_{Ry} = \rho^R(1 - \rho).$$

В качестве обслуживающего прибора в нашем случае выступает коллектив разработчиков, устраняющих выявленную в системе уязвимость с интенсивностью μ. На практике одновременно может устраняться несколько уязвимостей, т.е. в общем случае следует рассматривать схему "гибели и размножения" с *C* обслуживающими приборами. Для такой модели искомая характеристика определяется следующим образом[16]:

$$P_{0y} = (1 + \rho + \frac{\rho^2}{2!} + \cdots + \frac{\rho^C}{C!})^{-1},$$

а вероятность наличия в системе одновременно *R* не устраненных уязвимостей:

$$P_{Ry} = \frac{\rho^C}{C!} P_{0y}.$$

Отметим, что угроза уязвимости нами рассматривается (в данном случае моделируется) в качестве простейшего или базового элемента безопасности информационной системы. Далее потребуется моделирование уже более сложного элемента – угрозы атаки, создаваемой

угрозами уязвимости, а в конечном счете угрозы безопасности информационной системы в целом, создаваемой угрозами атак. С учетом этого для упрощения последующих моделей оценим, какое количество обслуживающих приборов С следует рассматривать при моделировании угрозы уязвимости и при каких условиях.

Можно предположить, что при условии $\rho = \frac{\lambda}{\mu} \ll 1$ значение вероятности $P_{R>1y}$мало и им можно пренебречь. Оценим влияние на результаты моделирования характеристики *C*, для чего рассмотрим изменение на интересующих нас интервалах значений характеристики P_{Ry} от изменения значений параметраρ для одноканальной, см. табл.1, и двух канальной (*C*=2), см. табл.2, систем.

Таблица 1

Характеристики одноканальной системы

P_{Ry}	ρ				
	0,1	**0,2**	**0,3**	**0,4**	**0,5**
P_{0y}	0,90	0,80	0,70	0,60	0,50
P_{1y}	0,09	0,16	0,21	0,24	0,25
$P_{R\geq 2y}$	0,01	0,04	0,09	0,16	0,25

Таблица 2

Характеристики двухканальной системы

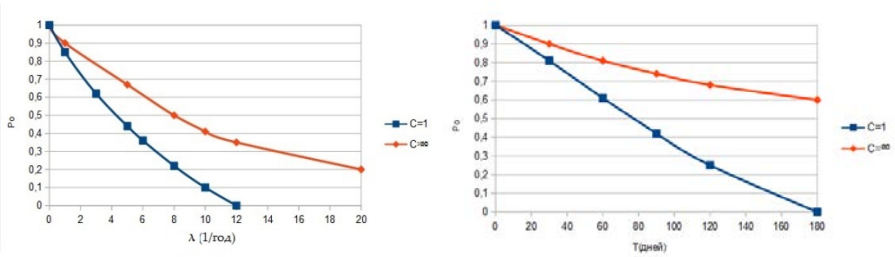
P_{Ry}	ρ						
	0,3	**0,4**	**0,5**	**0,6**	**0,7**	**0,8**	**0,9**
P_{0y}	0,74	0,68	0,60	0,56	0,51	0,47	0,43
P_{1y}	0,23	0,27	0,32	0,34	0,36	0,38	0,39
P_{2y}	0,03	0,05	0,08	0,10	0,13	0,15	0,18
$P_{R\geq 3y}$	0	0	0	0	0	0	0

Проанализировав результаты, представленные в табл.1 и в табл.2, можем сделать следующие выводы. При условии $\rho \leq 0{,}2$ при моделировании угрозы уязвимости может использоваться одноканальная схема "гибели и размножения", при условии же$\rho > 0{,}2$должна использоваться двухканальная схема.

Замечание.Условие $\rho > 0{,}9$ не анализируется, поскольку при выполнении данного условия о какой-либо безопасности говорить не приходится.

Использовав приведенную выше формулу, оценим влияние изменения значений параметров безопасности (интенсивности возникновения уязвимости λ и устранения уязвимости μ) на характеристику безопасности P_{0y}. Для этого рассмотрим, как изменяется

вероятность готовности информационной системы к безопасной эксплуатации в отношении угрозы уязвимости, причем будем рассматривать только одно программное средство, а не информационную систему в целом в зависимости от изменения продолжительности устранения разработчиком обнаруженных уязвимостей, при этом примем, что в программном средстве обнаруживается лишь одна уязвимость в год, см. рис.2.а; и как изменяется вероятность готовности информационной системы к безопасной эксплуатации в отношении угрозы уязвимости в зависимости от изменения интенсивности обнаружения уязвимостей в программном средстве, при этом примем, что среднее время устранения одной уязвимости составляет 1 месяц, см. рис.2.б [21].



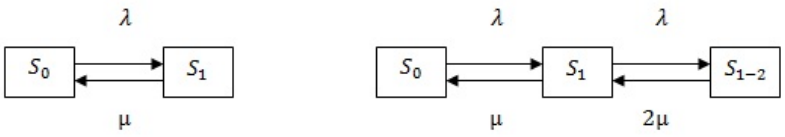
а. От продолжительности устранения одной обнаруженной уязвимости

б. От изменения интенсивности обнаруженияуязвимостей

Рис.2. Исследование изменения вероятности готовности информационной системы к безопасной эксплуатации в отношении угрозы уязвимости

Использовав данное исследование, обратившись вновь к рис.1, можем сделать вывод об очень низком уровне безопасности современных информационных систем, в которых как в системных средствах, так и в приложениях, уязвимости выявляются десятками в год.

Графы состояний случайного процесса выявления и устранения уязвимостей (марковского процесса с дискретными состояниями и непрерывным временем), которые нами далее будут использоваться, представлены на рис.3, где S_0 – исходное состояние системы, S_1 – в системе выявлена и не устранена одна из уязвимостей, S_{1-2} – в системе выявлены и не устранены две уязвимости.



а. При условии: $\rho \leq 0{,}2$ б. При условии: $\rho > 0{,}2$

Рис.3. Графы системы состояний случайного процесса для угрозы уязвимости

Теперь в двух словах о прогнозировании. Используя рассмотренный подход к моделированию характеристики угроз уязвимости, мы можем оценить ее значение лишь за

некоторый прошедший интервал времени, в то время как система защиты проектируются для использования в будущем, понятно, что необходимо прогнозирование.

В методическом плане основным инструментом любого прогноза является схема экстраполяции [17]. Сущность экстраполяции заключается в изучении сложившихся в прошлом и настоящем устойчивых тенденций развития объекта прогноза и в переносе их на будущее.

Различают формальную и прогнозную экстраполяцию. Формальная экстраполяция базируется на предположении о сохранении в будущем прошлых и настоящих тенденций развития объекта прогноза; при прогнозной экстраполяции фактическое развитие увязывается с гипотезами о динамике исследуемого процесса с учетом изменений влияния различных факторов в перспективе.

Методы экстраполяции сегодня являются наиболее распространенными и проработанными. Основу экстраполяционных методов прогнозирования составляет изучение эмпирических рядов. Эмпирический ряд — это множество наблюдений, полученных последовательно во времени. В прогнозировании широко применяется метод математической экстраполяции, в математическом смысле означающий распространение закона изменения функции из области ее наблюдения на область, лежащую вне отрезка наблюдения. Функция представляет собой математико-статистическую модель, отражающую зависимость объекта прогнозирования от влияющих на него факторов. Результат при этом связывается исключительно с ходом времени. Предполагается, что через время можно выразить влияние всех основных факторов.

Экстраполяция базируется на следующих допущениях:

1) развитие явления может быть с достаточным основанием охарактеризовано плавной (эволюторной) траекторией — трендом;
2) общие условия, определяющие тенденцию развития в прошлом, не претерпят существенных изменений в будущем, т.е. предполагается определенная консервативность поведения явления.

Для экстраполяциихарактерно нахождение плавной линии, отражающей закономерности развития во времени или так называемой линии теоретического тренда. Тренд экстраполируемого явления – это длительная тенденция изменения показателей, т.е. изменение, определяющее общее направление развития, основную тенденцию временных рядов.

Разработка прогноза заключается в определении вида экстраполирующей функции на основе исходных эмпирических данных и параметров [17]. Первым этапом является выбор оптимального вида функции, дающей наилучшее описание тренда. Следующим этапом является расчет параметров выбранной экстраполяционной функции.

В общем случае экстраполяция на основе тренда включает:

- сбор информации по динамическому ряду показателя, характеризующего изучаемое явление, за прошлые периоды;
- выбор оптимального вида функции, описывающей указанный ряд путем его сглаживания и выравнивания (аппроксимация);
- расчёт параметров выбранной аппроксимирующей функции;
- расчёт прогноза на будущее по выбранной функции путем ее экстраполяции.

При оценке параметров зависимостей наиболее распространенными являются метод наименьших квадратов, метод экспоненциального сглаживания временных рядов, метод скользящей средней и другие.

Естественно, что о прогнозной экстраполяции речь можно вести лишь при условии достаточности накопленной статистики, в нашем случае при условии оценки параметров угроз уязвимостей (соответствующих групп уязвимостей) за достаточно продолжительное время, по крайней мере, за несколько лет. При отсутствии подобной статистики, что в отношении многих типов уязвимостей имеет место на практике, целесообразно воспользоваться формальной экстраполяцией, т.е. сделать предположение о сохранении в будущем периоде эксплуатации системы рассчитанных параметров соответствующих угроз уязвимостей, исходя из имеющегося краткосрочного периода наблюдений.

Поскольку использование формальной экстраполяции при прогнозировании может привести к значительной погрешности в сделанных прогнозах, как следствие, этот подход требует накопления статистики в отношении изменения параметров соответствующих угроз уязвимостей на последующих этапах эксплуатации системы с последующей корректировкой сделанных прогнозов с возможностью в некоторых случаях перехода к прогнозной экстраполяции.

Ранее, обосновывая корректность использования при моделировании марковских процессов, мы показали, что со временем последующей эксплуатации системы защитырасчетное значение ее характеристики безопасности хуже не будет. Однако существует еще задача прогнозирования появления новых типов уязвимостей.

К сожалению, именно формальная экстраполяция может применяться в отношении прогноза типов угроз уязвимостей, которые могут быть выявлены на последующих этапах эксплуатации защищенной информационной системы. Использование прогнозной экстраполяции с целью предсказания появления новых типов уязвимостей не представляется возможным.

Все это обусловливает необходимость постановки и рассмотрения задачи проектирования системы защиты информационной системы как непрерывного процесса,

предполагающего корректировку прогнозов,в первую очередь в отношении учета появления новых типов уязвимостей на последующих этапах эксплуатации системы.

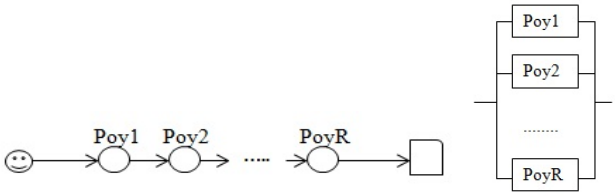
1.3. Интерпретация и марковскиемодели угрозы атаки на информационную систему

1. Интерпретация угрозы атаки.

Говоря об угрозе атаки, прежде всего напомним, что информационная безопасность имеет несколько ключевых характеристик, к которым относятся конфиденциальность, целостность и доступность обрабатываемой информации [1]. Атака на информационную систему реализуется с целью нарушения, как правило, одной из этих характеристик – с учетом этого строится и защита информационной системы в зависимости от ее назначения: защита от нарушения конфиденциальности информации (защита от ее хищения), защита от нарушения целостности информации (защита от ее несанкционированной модификации), защита от нарушения доступности информации. Естественно, говоря далее об угрозе атаки, подразумеваем, что эта атака может быть реализована нарушителем с определенной целью.

В [22] угрозу атаки на информационную систему было предложено представлять соответствующим орграфом, проиллюстрированным на рис.4.а, где через P_{0yr}, $r=1,\ldots,R$, обозначается вероятность отсутствия в системе r-й уязвимости (информационная система готова к безопасной эксплуатации в отношении угрозыr-й уязвимости) – одной из R реальных угроз уязвимостей, последовательно (дуги графа определяют последовательность использования выявленных уязвимостей при реализации атаки) используемых атакой на информационную систему.

При подобном представлениии угроза атаки на информационную систему может интерпретироваться схемой параллельного резервирования угроз уязвимостей, резервируемыми и резервирующими элементами которой являются угрозы уязвимости[22], см. рис.4.б, поскольку каждая угроза уязвимости, присутствующая в системе с вероятностью P_{0yr}, может рассматриваться в качестве резервирующего элемента (с вероятностью P_{0yr} предотвращает атаку).



а. Орграф угрозы атаки б. Схема параллельного резервирования

Рис.4. Орграф угрозы атаки и ее интерпретация схемой параллельного резервирования угроз уязвимостей

Данная интерпретация позволяет представлять систему защиты информационной системы в виде отдельной вершины (отдельных вершин) на орграфе угрозы атаки с параметрами безопасности $\lambda_{\text{сзи}}$ и $\mu_{\text{сзи}}$ уже собственно системы защиты (это параметры угроз уязвимостей системы защиты).Подобная интерпретация угрозы атаки позволяет сделать важнейший вывод о том, что угрозы уязвимостей, создающие угрозу атаки, с точки зрения их нивелирования системой защиты эквивалентны, поскольку при нивелировании любой из них угрозы системы защиты включаются в схему параллельного резерва,см. рис.2.б, одинаково с параметрами безопасности системы защиты $\lambda_{\text{сзи}}$ и $\mu_{\text{сзи}}$.

Если обозначить вероятность того, что система защиты, используемая для нивелирования уязвимости, готова к безопасной эксплуатации, через $P_{0\text{сзи}}$, то вероятность того, что защищенная в отношении угрозы уязвимости информационная система будет готова к безопасной эксплуатации, $P_{0\text{узис}}$ при использовании системы защиты, нивелирующей эту угрозу уязвимости, может быть определена следующим образом:

$$P_{0\text{узис}} = 1 - \left(1 - P_{0\text{у}}\right)(1 - P_{0\text{сзи}}),$$

а вероятность того, что защищенная информационная система готова к безопасной эксплуатации, $P_{0\text{азис}}$ в отношении угрозы атаки при использовании системы защиты, нивелирующей одну из R уязвимостей, используемых атакой:

$$P_{0\text{азис}} = 1 - (1 - P_{0\text{сзи}}) \prod\nolimits_{r=1}^{R} (1 - P_{0\text{у}r})$$

Отметим, что данная формула, соответствующая схеме параллельного резерва, верна только в том случае, если резервируемый элемент (угроза атаки на информационную систему) и резервирующий ее элемент (угроза атаки на систему защиты) не зависимы по угрозам уязвимостей. Если же эти угрозы атак на информационную систему и на систему защиты создаются одними и теми же угрозами уязвимостей, то данные угрозы уязвимости должны интерпретироваться схемой последовательного резервирования.

С учетом сказанного можем сделать важный вывод, заключающийся в формировании важнейшего требования к системе защиты.

Вывод.

Угрозы атак на информационную систему и на систему защиты должны быть независимы по угрозам уязвимостей. Обеспечение независимости угроз атак на информационную систему и на систему защиты по угрозам уязвимостей можно позиционировать в качестве фундаментального требования к средству защиты при его проектировании.

Замечание. Данный важный вывод позволяет пересмотреть и требования к резервированию элементов информационной системы, показав, что известные из теории надежности методы резервирования в информационной безопасности в общем случае не применимы. Эти вопросы будут исследованы в третьем разделе учебного пособия.

При полной зависимости угроз атак на информационную систему и на систему защиты по угрозам уязвимости резервирование (защита) не осуществляется, т.е. для $P_{0\text{азис}}$ имеем:

$$P_{0\text{азис}} = 1 - \prod_{r=1}^{R} (1 - P_{0\text{у}r})$$

Все сказанноеможно отнести и к вопросам резервирования собственно систем защиты. Резервирование систем защиты – параллельное резервирование,используется для повышения (обеспечения требуемого) уровня информационной безопасности в отношении угрозы атаки, реализуется нивелированием различными системами защиты нескольких угроз уязвимостей, создающих угрозуодной атаки, либо различными системами защиты одной угрозы уязвимости (в обоих случаях реализуется параллельное резервирование угроз уязвимостей).

Замечание. Под различными системами защиты здесь понимаем системы, не зависимые между собою по угрозам уязвимостей.

При подобном резервировании систем защиты каждая из них будет включаться в качестве параллельного резерва по схеме, представленной на рис.4.б. При использовании для защиты от угрозы атаки одновременно *M* различных систем защиты с номерами *m=1,…,M,* характеризуемых вероятностями того, что *m*-е средство защиты готово к безопасной эксплуатации через $P_{0\text{сзи}m}$, получаем формулу расчета данной характеристики с параллельным резервированием в информационной системе систем защиты:

$$P_{0\text{азис}} = 1 - \prod_{r=1}^{R} (1 - P_{0\text{у}r}) \prod_{m=1}^{M} (1 - P_{0\text{сзи}m})$$

Замечание. В случае если резервируемые системы защиты зависимы по угрозам уязвимостей (атака на одну и ту же уязвимость позволяет преодолеть резервируемые системы защиты), в отношении этих угроз уязвимостей реализуется последовательное резервирование (отказ элемента приводит к отказу всей резервируемой системы). Пусть зависимых угроз уязвимости в *M* различных средствах защиты с номерами *m=1,…,M* равно *Dm* с номерами *dm=1,...,Dm* (любая из этих угроз уязвимостей может присутствовать во всех средствах защиты *M*), характеризуемых $P_{0\text{у}rdm}$, кроме того, пусть каждое из *M* средств защиты характеризуется *Gm* уникальными угрозами уязвимостей с номерами *gm=1,...,Gm*, характеризуемых $P_{0\text{у}rgm}$, для простоты опять же предположим, что успешная атака на каждую подобную уязвимость приводит к успешной атаке на средство защиты в целом (угрозы уязвимостей средства защиты не рассматриваются в качестве параллельного резерва – угроза уязвимости является угрозой

атаки). В данных предположениях характеристика угрозы атаки на зарезервированную систему защиты $P_{0\text{асзи}}$ имеет следующий вид:

$$P_{0\text{асзи}} = (1 - \prod_{m=1}^{M}(1 - \prod_{gm=1}^{Gm} P_{0\text{у}rgm}))\prod_{dm=1}^{Dm} P_{0\text{у}rdm}$$

Заметим, что, если в данных предположениях в M различных системах защиты с номерами $m=1,\ldots,M$отсутствуют зависимые угрозы уязвимости систем защиты $Dm=0$, имеем:

$$P_{0\text{асзи}} = (1 - \prod_{m=1}^{M}(1 - \prod_{gm=1}^{Gm} P_{0\text{у}rgm}))$$

В случае же, если в данных предположениях в M различных системах защиты с номерами $m=1,\ldots,M$присутствуют только зависимые угрозы уязвимости систем защиты $Gm=0$, имеем:

$$P_{0\text{асзи}} = \prod_{dm=1}^{Dm} P_{0\text{у}rdm}$$

Т.е. как такого резервирования систем защитыв этом случае не осуществляется.

Теперь остановимся на вопросах нивелирования угрозы уязвимости системой защиты с целью обоснования того, каким способом должна решаться данная задача. Например, выше была рассмотрена возможность защиты от вредоносных программ, основанная на предотвращении возможности, в том числе и системными правами, исполнения в системе создаваемых в процессе работы интерактивными пользователями файлов [24]. Это пример нивелирования (устранения как таковой) технологической уязвимости (недоработки защиты современных ОС). Решается данная задача методами контроля и разграничения прав доступа к защищаемым объектам.

Сегодня на практике широко распространеныальтернативные решения, не предполагающие нивелирования (устранения) угроз уязвимостей. К таким решениям можно, например, отнести антивирусные средства защиты– решения, основанные на анализе каких-либо контролируемых событий на соответствие неким эталонным множествам (например, сигнатурный и/или поведенческий анализ). Поскольку данные эталонные множества априори не могут быть полными,создаваемая в системе уязвимость всегда выявляется лишь с некоторой вероятностью, причем зависящей от полноты эталонного множества событий, как следствие, значение параметра $\lambda_{\text{сзи}}$растет по мере эксплуатации системы защиты.

Замечание. Из сказанного следует, что использование марковских процессов для моделирования подобных систем позволяет отыскать не худшее, а лучшее значение соответствующей характеристики безопасности, т.е. граничное значение, задающее условие "будет только хуже".

Как ранее отмечали, важнейшее достоинство прогнозной экстраполяции состоит в выявлении ключевых тенденций анализируемого явления, позволяющих делать

соответствующие обоснованные выводы и предположения. Проиллюстрируем сказанное примером. Еще в 2009 году экспертами был сделан прогноз в отношении роста вирусной активности, см. рис.5, в результате которого сделан вывод в отношении того, что в ближайшие годы вирусная активность будет только значительно возрастать, и в 2015 году количество новых вредоносных программ может превысить 200 млн.[32]. На основании данного прогноза, основанного на выявлении соответствующего тренда, в [32] сделан еще один куда более важный вывод о технологическом тупике существующих антивирусных технологий защиты, в частности о необходимости разработки принципиально иных технологий защиты от вредоносных программ.

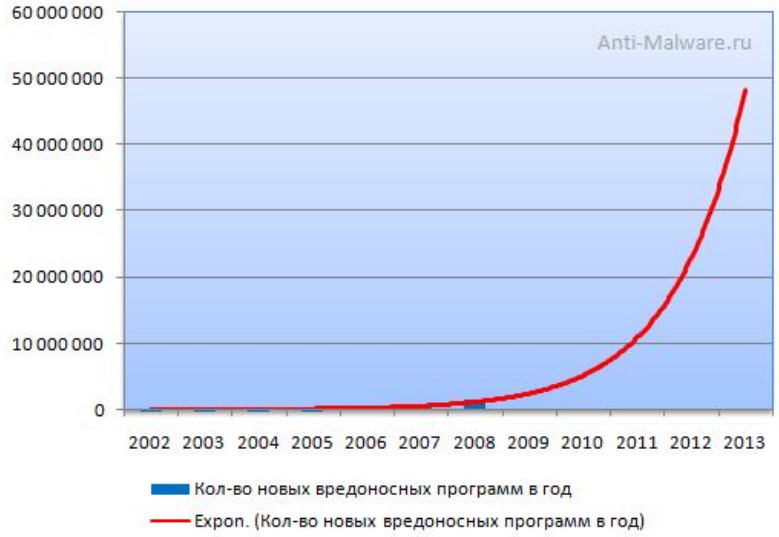


Рис.5. Прогноз роста вирусной активности

К сожалению, за прошедшие годы новых технологий антивирусной защиты (по крайней мере, в широком использовании) не появилось. Оценим (по прошествии пяти лет), насколько оправдался данный прогноз. Эксперты из ИБ-компании PandaSecurity опубликовали отчет о киберугрозах за первый квартал 2014 года [33]. Согласно документу, указанный период является рекордным по количеству вредоносных программ, создаваемых ежедневно. Так, по данным экспертов, в первом квартале зафиксировано более 15 млн. новых образцов вредоносных программ–число создаваемых вредоносных программ составило около 160 тысяч в день. Как видим, прогноз во многом оправдался.

По самым оптимистичным прогнозам современными антивирусными средствами защиты выявляется до 75% новых вредоносных программ, а интенсивность создания новых вредоносных программ, как показали выше, определяется десятками, если уже не сотнями миллионов в год.С учетом сказанного не сложно рассчитать $\lambda_{\text{сзи}}$подобных современных средств защиты. Задавая различные расчетные значения$\mu_{\text{сзи}}$ (а это, по крайней мере, единицы, а то и десятки дней, ведь мы говорим о тех вредоносных программах, которые не выявляются

антивирусным средством защиты, их еще нужно каким-то образом обнаружить), можно легко определить, сколько обслуживающих приборов (в данном случае одновременно работающих над различными сигнатурами вирусных аналитиков С) потребуется антивирусной компании для выполнения требования к стационарности системы. Напомним, условие стационарности системы массового обслуживания в рассматриваемом случае:$\frac{\lambda_{\text{сзи}}}{C\mu_{\text{сзи}}} < 1$[16].Как отмечали, число создаваемых новых вредоносных программ составляет около 160 тысяч в день (и продолжает расти), детектируется из них 75%. Это означает, что ежедневно антивирусная компания для выполнения требования к стационарности системы (число заявок на обслуживание не возрастает до бесконечности) должна обрабатывать 40 тысяч вредоносных программ в день.К слову сказать, из этого анализа можем сделать вывод о том, что основными характеристиками эффективности защиты в данном случае является не интенсивность выявления сигнатуры вируса $\mu_{\text{сзи}}$, а средняя длина очереди заявок на облуживание (выявленных вредоносных программ) и среднее время пребывание заявки на обслуживание в очереди, поскольку система не стационарна.А ведь мы еще не анализируем задачу выявления новой вредоносной программы, не детектируемой антивирусным средством защиты.Здесь мы получили лишь грубую оценку, поскольку, как отмечали, для моделирования подобных систем марковские процессы уже не применимы. Однако и такая грубая оценка объясняет столь стремительный рост числа создаваемых вредоносных программ, см. рис.5, вызванный крайне низкой эффективностью существующих антивирусных средств защиты, и позволяет сделать соответствующий важнейший вывод.

Есть и еще одна ключевая проблема антивирусных средств защиты, о которой следует упомянуть. Естественно, что объем базы сигнатур растет пропорционально росту новых обнаруживаемых вредоносных программ. Для того чтобы проверить некий файл на наличие в нем вируса (потенциальной вредоносной активности), необходимо этот файл при каких либо условиях (например, перед попыткой исполнения, при записи на компьютер и т.д.) сравнить со всеми сигнатурами в базе на совпадение. Естественно, что это не может не сказаться на значительной загрузке вычислительного ресурса, причем эта загрузка будет тем существенней, чем больше объем базы сигнатур, а стремительность роста числа новых создаваемых ежедневно вредоносных программ мы уже иллюстрировали. Конечно, уже давно пора задуматься о технологическом тупике существующих антивирусных технологий защиты и искать новые технологии защиты.

Вывод.

Эффективная защита может быть реализована только методами защиты, реализующими нивелирование угрозы уязвимости, т.е. методами контроля и разграничения прав доступа к защищаемым объектам.

Теперь оценим потенциальные возможности реализации эффективной защиты с использованием систем защиты, нивелирующих угрозы уязвимости, основанных на реализации разграничительной политики доступа к ресурсам [28]. С этой целью получим и проанализируемзначения характеристики $P_{0у}$,собственно средства защиты $P_{0усзи}$ при различных значениях$\lambda_{сзи}$ и $\mu_{сзи}$ (поскольку нас интересует условие $\rho \leq 0{,}2$, то для расчетов используем модель, приведенную на рис.3.а).Расчетные значения приведены в табл.3.

Таблица 3

Оценка уровня эксплуатационной информационной безопасности защищенной информационной системы

Интенсивность устранения выявленных уязвимостей в системе защиты $\mu_{сзи}$	**Вероятность готовности к безопасной эксплуатации средства защиты $P_{0усзи}$при различных интенсивностях выявления уязвимостей в системе защиты $\lambda_{сзи}$**			
	1/ 3 месяца	**1/ 6 месяца**	**1/ 12 месяца**	**1/ 18 месяца**
1/3 дня	0,97	0,98	0,99	0,99
1/7 дней	0,93	0,96	0,98	0,99
1/14 дней	0,87	0,93	0,96	0,98

Проведем анализ полученных результатов. Исходя из существующей практики внедрения и технического обслуживания систем защиты информации, можем заключить, что требование к продолжительности устранения выявленной уязвимости на практике (требование из технического задания на техническое сопровождение системы защиты) составляет не более 1 недели (7 дней). Как видим из табл.3, в этих условиях для обеспечения $P_{0сзи}$= 0,93 допустимо выявление в год в среднем 3,33 уязвимости, для обеспечения $P_{0сзи}$= 0,96 допустимо выявление в год в среднем 2 уязвимости, для обеспечения $P_{0сзи}$ = 0,98 допустимо выявление в год в среднем 1 уязвимости.

Из сказанного можно сделать вывод, что обеспечение вероятности готовности к безопасной эксплуатации системы защиты 0,9и выше достижимо на практике.

Теперь оценим, какое значение вероятности готовности к безопасной эксплуатации защищенной информационной системы $P_{0азис}$достигается при использовании в ней системы

защиты, характеризуемой условием $P_{0сзи}$= 0,98, при различных значениях характеристики$P_{0а}$для угрозы атаки защищаемой информационной системы, см. табл.4. Для расчетов используем следующую формулу:

$$P_{0азис} = 1 - (1 - P_{0сзи})(1 - P_{0а})$$

Таблица 4

Оценка изменения характеристики $P_{0азис}$ от изменен я характеристики $P_{0а}$ при $P_{0сзи}$ = 0,98

Вероятность готовности информационной системы к безопасной эксплуатации в отношении угрозыатаки $P_{0а}$								
	0,0	**0,1**	**0,2**	**0,3**	**0,4**	**0,5**	**0,6**	**0,7**
$P_{0азис}$	0,980	0,982	0,984	0,986	0,988	0,99	0,992	0,994

Теперь рассмотрим обратную задачу. Используя ту же формулу, оценим, как будет изменяться требование к характеристике системы защиты $P_{0сзи}$ при изменении значения вероятности готовности информационной системы к безопасной эксплуатации в отношении угрозы атаки$P_{0а}$, при необходимости обеспечения в информационной системе значения вероятности готовности к безопасной эксплуатации защищенной информационной системы$P_{0азис}$= 0,98. Соответствующие расчеты представлены в табл.5.

Таблица 5

Оценка изменения характеристики $P_{0сзи}$ от изменения характеристики $P_{0а}$ при $P_{0азис}$ = 0,98

Вероятность готовности системы защиты к безопасной эксплуатации в отношении угрозы атаки$P_{0а}$								
	0,0	**0,1**	**0,2**	**0,3**	**0,4**	**0,5**	**0,6**	**0,7**
$P_{0сзи}$	0,980	0,978	0,975	0,971	0,967	0,96	0,950	0,933

Из проведенных исследований, результаты которых приведены в табл.4, табл.5, видим, что изменение значения вероятности готовности информационной системы к безопасной эксплуатации в отношении угрозы атаки $P_{0а}$ достаточно сильно влияет на требование к характеристике безопасности системы защиты $P_{0сзи}$, что соответствующим образом должно учитываться при проектировании системы защиты информационной системы.

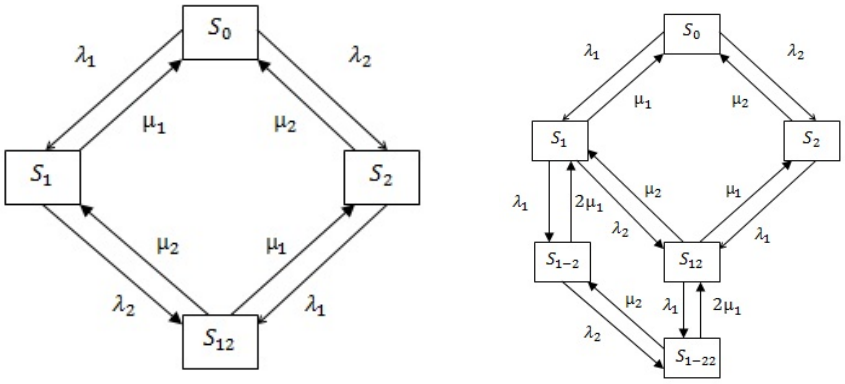
Из проведенного исследования можно сделать вывод о том, что потенциально высокое значение характеристики безопасностисистем защиты, решающих задачу нивелирования уязвимостей, достижимо. Требования к характеристике безопасности системы защиты (в конечном счете к значениям его параметров безопасности $\lambda_{сзи}$ и $\mu_{сзи}$) могут формулироватьсяв результате еепроектирования. Причем оценить выполнимость данных требований на практике

достаточно просто, используя соответствующую статистику выявления и устранения уязвимостей в системе защиты в процессе ее эксплуатации.

2. Марковская модель угрозы атаки как системы с отказами и восстановлениями характеристики безопасности.

Информационную систему как в отношении возникновения и устранения угрозы уязвимости, так и в отношении возникновения и устранения угрозы атаки в целом, создаваемой соответствующей совокупностью угроз уязвимостей, можно рассматривать как систему с отказами и восстановлениями, в нашем случае – характеристики безопасности.

Построим марковскую модель, описывающую процесс возникновения и устранения реальной угрозы атаки в информационной системе. С этой целью рассмотрим математическое описание марковского процесса с дискретными состояниями и непрерывным временем на примере орграфа угрозы атаки, содержащего (для простоты иллюстрации) две взвешенные вершины уязвимостей: угроза атаки создается двумя угрозами уязвимости с соответствующими им параметрами – интенсивностями выявления и устранения уязвимостей. Сначала предположим, что для обеих угроз уязвимостей выполняется условие$\rho \leq 0{,}2$. Граф системы состояний случайного процесса (марковского процесса) представлен на рис.6.а. На графе представлены четыре возможных состояния системы: S_0 – исходное состояние системы, S_1 – в системе выявлена и не устранена первая уязвимость, S_2 – в системе выявлена и не устранена вторая уязвимость, S_{12} – в системе выявлены и не устранены обе уязвимости– создана реальная угроза атаки.Естественно полагаем, что все переходы системы из одного состояния в другое происходят под воздействием простейших потоков событий с соответствующими интенсивностями выявления или устранения уязвимостей.



а. При условии:$\rho \leq 0{,}2$б. При условии:$\rho > 0{,}2$

Рис.6. Графы системы состояний случайного процесса для угрозы атаки

Система дифференциальных уравнений Колмогорова для вероятностей состояний для данного графа будет иметь следующий вид:

$$\begin{cases} P_0' = \mu_1 P_1 + \mu_2 P_2 - (\lambda_1 + \lambda_2) P_0 \\ P_1' = \lambda_1 P_0 + \mu_2 P_3 - (\lambda_2 + \mu_1) P_1 \\ P_2' = \lambda_2 P_0 + \mu_1 P_3 - (\lambda_1 + \mu_2) P_2 \\ P_{12}' = \lambda_2 P_1 + \lambda_1 P_2 - (\mu_1 + \mu_2) P_{12} \end{cases}$$

Заменяя в уравнениях Колмогорова их производные нулевыми значениями, получим систему линейных алгебраических уравнений, описывающих стационарный режим, решая которую, с учетом полноты группы событий, т.е., используя условие:

$$P_0 + P_1 + P_2 + P_{12} = 1,$$

находим искомые предельные (или финальные) вероятности состояний.

Применительно к рассматриваемой задаче моделирования интерес представляет состояние S_{12} – в системе выявлены обе уязвимости, характеризуемое вероятностью P_{12} – это состояние, в котором создаются условия для осуществления атаки (создается реальная угроза атаки), поскольку выявлены и не устранены все уязвимости, необходимые для осуществления атаки.

Таким образом, эту характеристику можем далее рассматривать в качестве вероятности возникновения угрозы атаки ($P_{\text{уа}} = P_{12}$). Соответственно вероятность готовности к безопасной эксплуатации системы в отношении угрозы атаки P_{0a} (или стационарный коэффициент готовности $К_г$) определяется следующим образом:

$$К_г = P_{0a} = P_0 + P_1 + P_2$$

Замечание. Для графа, представленного на рис.6.а, $К_г$ рассчитывается по следующей формуле:

$$К_г = \frac{\mu_1\mu_2 + \lambda_1\mu_2 + \lambda_2\mu_1}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)}$$

Привыполнения условия $\rho > 0{,}2$ для угрозы какой-либо уязвимости в граф системы состояний случайного процесса для угрозы атаки должен включаться соответствующий граф, описывающий процесс возникновения и устранения подобной уязвимости, см. рис.3.б. Каким образом это делается проиллюстрировано на рис.6.б (в предположении, что данное условие выполняется для угрозы первой уязвимости).

Как видим, для расчета значений характеристики угрозы атаки здесь не требуется использования каких-либо экспертных оценок. Адекватность подобной модели угрозы атаки обусловливается использованием объективных значений требуемых для проведения расчетов параметров угроз уязвимостей, получаемых на основании существующей их статистики.

3. Укрупненная марковская модель угрозы атаки как системы с отказами и восстановлениями характеристики безопасности.

Построение укрупненной модели угрозы атаки необходимо для расчета следующих важнейших характеристик угрозы атаки: интенсивности возникновения $\boldsymbol{\lambda}_{\text{а}}$ и интенсивности

устранения μ_a реальной угрозы атаки, а также среднего времени наработки на отказ (восстанавливаемая система) характеристики безопасности $\boldsymbol{T_{0\text{уа}}}$, определяющего средний интервал времени между отказами характеристики безопасности–моментами возникновениями реальной угрозы атаки. Основу построения укрупненной модели составляет использование параметра потока отказов [14].

В марковских моделях надежности параметр потока отказов ω определяется (для стационарного участка) следующим образом:

$$\boldsymbol{\omega} = \sum_{i \epsilon Q_+} \boldsymbol{P_i} \sum_{j \epsilon Q_-} \boldsymbol{\lambda_{ij}},$$

где $\boldsymbol{Q_+}$– множество состояний работоспособности системы, $\boldsymbol{Q_-}$– множество состояний отказа системы, $\boldsymbol{\lambda_{ij}}$ – интенсивность перехода из *i*-го работоспособного состояния, вероятность нахождения в котором системы $\boldsymbol{P_i}$, в*j*-е неработоспособное состояние.

Параметр потока отказов, характеризующий частоту возникновения событий отказа в восстанавливаемых системах, обратно пропорционален среднему времени между отказами $T_{\text{моа}}$, в западной литературе используется аббревиатура MTBF (Mean Time Between Failures),строгое доказательство этого отношения приведено в теории восстановления:

$$T_{\text{моа}} = \frac{1}{\omega} = T_{0\text{уа}} + T_{\text{в}},$$

где $T_{\text{в}}$ – среднее время восстановления.

Исходя из того, что

$$\text{К}_\text{г} = \frac{T_{0\text{уа}}}{T_{0\text{уа}} + T_{\text{в}}},$$

имеем

$$T_{0\text{уа}} = \text{К}_\text{г}/\omega.$$

Для построения укрупненной модели угрозы атаки вновь обратимся к графу, представленному на рис.6.а, и определимся с тем, как формируется поток отказов характеристики безопасности и каким образом определить его эффективность. Как видим, угроза атаки создается в двух случаях: при переходе из состояния S_1, в котором система находится с вероятностью P_1(в марковской модели вероятность состояния интерпретируется как относительная доля времени нахождения системы в этом состоянии),в состояние S_{12} (это состояние реальной угрозы атаки) переходы осуществляются с интенсивностью λ_2 (с учетом же соответствующей доли времени нахождения в состоянии S_1 – с интенсивностью $P_1\ \lambda_2$),и при переходе из состояния S_2, в котором система находится с вероятностью P_2, в состояние S_{12} переходы осуществляются с интенсивностью λ_1(с учетом же соответствующей доли времени нахождения в состоянии S_2 – с интенсивностью $P_2\ \lambda_1$). В нашем случае определяемый подобным образом поток отказов может интерпретироваться как поток возникновения реальной угрозы атаки с интенсивностью λ_a:

$$\lambda_{\text{а}} = \omega = P_1\,\lambda_2 + P_2\,\lambda_1$$

Укрупненная модель угрозы атаки описывается графом, приведенным на рис.3.а, в котором соответствующим образом $\lambda_{\text{а}}$ и $\mu_{\text{а}}$ определяются интенсивности переходов, состояние S_0 соответствует отсутствию, а S_1 – возникновению реальной угрозы атаки. Остальные искомые характеристики угрозы атаки рассчитываются по следующим формулам:

$$T_{0\text{уа}} = 1/\lambda_{\text{а}}$$

$$\mu_{\text{а}} = \frac{\lambda_{\text{а}} К_{\text{г}}}{1 - К_{\text{г}}} = 1/T_{\text{в}}$$

Рассмотренные марковские модели могут применяться при общей оценке свойств безопасности отдельных средств, в том числе и систем защиты, приложений и информационных систем. При проектировании же системы защиты информационной системы, при оценке уровня безопасности какой-либо конкретной информационной системы, используемой для обработки определенной информации, необходимо учитывать готовность реализации создаваемой в системе реальной угрозы атаки нарушителем, что во многом обусловливается субъективными факторами, определяющими заинтересованность нарушителя в реализации соответствующей атаки на соответствующую информационную систему. Это можно отнести к принципиальным отличиям задачи моделирования в области информационной безопасности от соответствующих задач моделирования в теории надежности.

4. Марковские модели угрозы атаки как системы с отказами, восстановлениями и фатальным отказом характеристики безопасности.

Ранее применительно к угрозе уязвимости и к угрозе атаки мы говорили о системе с отказами и восстановлениями характеристики безопасности. Введем понятие фатального отказа– отказа характеристики безопасности, под которым будем понимать успешную реализацию нарушителем атаки на информационную систему. В результате подобного отказа нарушителем осуществляется несанкционированный доступ к информации (в первую очередь нас здесь интересует нарушение доминирующей характеристики безопасности– нарушение конфиденциальности информации), как следствие, в отношении подобного фатального отказа характеристики безопасности система уже может рассматриваться как невосстанавливаемая– конфиденциальность информации нарушена.

Замечание. В части иных характеристик безопасности – нарушение целостности и доступности информации – также будем использовать понятие фатального отказа с той лишь разницей, что в данном случае, в отличие от нарушения конфиденциальности информации, будем говорить о восстанавливаемом фатальном отказе (восстановление целостности информации, например, из резервной копии или ее доступности, например, переустановка системных средств или приложений).

Состояние фатального отказа в марковской модели угрозы атаки может быть учтено с использованием поглощающего состояния (состояния, не имеющего выхода). Введем понятие коэффициента готовности реализации нарушителем реальной угрозы атаки, обозначим его через $К_{га}$, который имеет физический смысл вероятности того, что создаваемая в системе реальная угроза атаки будет реализована нарушителем. Граф системы состояний случайного процесса (марковского процесса), соответствующий системе, граф которой представлен на рис.6.а, ноуже с фатальным отказом представлен на рис.7.

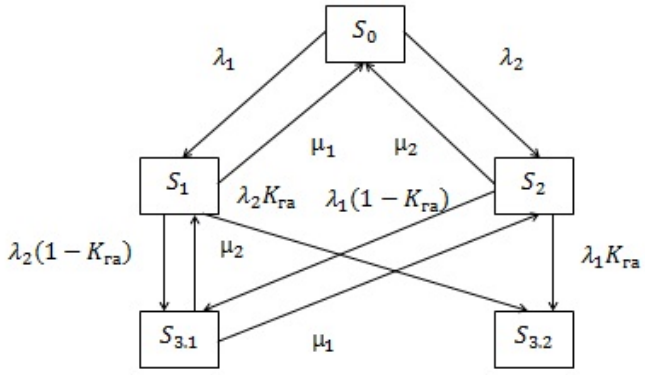


Рис.7. Граф системы состояний случайного процесса для угрозы атаки с фатальным отказом

При возникновении условия реализации атаки: реальная угроза атаки ($P_{уа} = 1$, соответственно $P_{0a} = 0$), атака будет реализована потенциальным нарушителем с вероятностью $K_{га}$, с вероятностью же $1 - K_{га}$ атаки не произойдет. Это учитывается включением в граф системы состояний случайного процесса, представленный на рис.6.а, вместо состоянияS_{12} двух состояний$S_{3.1}$ и $S_{3.2}$, см. рис.7. Переход в состояние$S_{3.1}$ предполагает неготовность совершения атаки нарушителем при возникновении ее реальной угрозы (поэтому для этого состояния присутствуют переходы в состояния S_1 и S_2). Переход в состояние $S_{3.2}$ – поглощающее состояние, характеризует реализацию атаки нарушителем на информационную систему.

Вероятность готовности к безопасной эксплуатации системы в отношении угрозы атаки $P_{0а}$ (или стационарный коэффициент готовности$K_г$) в данном случае определяется следующим образом:

$$K_г = P_{0a} = P_0 + P_1 + P_2 + P_{3.1}$$

Как ранее отмечали, значение вероятностиP_iсостояния (как предельной вероятности) в марковской модели показывает среднее относительное время пребывания системы в i–м состоянии. В данном случае эти вероятности рассчитываются также, как было описано ранее (с учетом того, что из поглощающей вершины нет выхода). Отличие состоит в интерпретации вероятности $P_{уа}$ ($P_{уа} = P_{3.2}$). В данном случае это вероятность реализации успешной атаки на информационную систему.Для вычисления среднего абсолютного времени пребывания

системы в каждом i-м состояний T_i в системе уравнений Колмогорова нужно положить нулю все производныеP_i' (P_i'=0), кроме P_0', если считать, что в начальный момент вероятность первого состояния P_0 =1. Тогда на основании теоремы о дифференцировании изображений в преобразовании Лапласа правая часть первого уравнения будет равна –1. В правых частях уравнений вместо P_iподставляются T_i, и относительно них решается система алгебраических уравнений.

С учетом сказанного, для рассматриваемого примера применительно к графу, приведенному на рис.7, например, для простоты – для случая$К_{га} = 1$ (отсутствует вершина $S_{3.1}$, вершину же $S_{3.2}$ обозначим как S_3) получаем:

$$\begin{cases} -1 = \mu_1 T_1 + \mu_2 T_2 - (\lambda_1 + \lambda_2) T_0 \\ 0 = \lambda_1 T_0 + \mu_2 T_3 - (\lambda_2 + \mu_1) T_1 \\ 0 = \lambda_2 T_0 + \mu_1 T_3 - (\lambda_1 + \mu_2) T_2 \\ 0 = \lambda_2 T_1 + \lambda_1 T_2 - (\mu_1 + \mu_2) T_3 \end{cases}$$

Рассчитав же значения T_i и просуммировав их для состояний, не являющихся поглощающими, можем вычислить важнейшую характеристику –среднее время наработки системы до отказа характеристики безопасности (система с фатальным отказом) – до реализации на нее успешной атаки(реализации угрозы атаки)нарушителем $T_{д0уа}$. Например, для системы, описываемой графом, представленным на рис.7, $T_{д0уа}$ определяется следующим образом:

$$T_{д0уа} = T_0 + T_1 + T_2 + T_{3.1}$$

Граф системы состояний случайного процесса (марковского процесса) укрупненной марковской модели угрозы атаки как системы с отказами, восстановлениями и фатальным отказом характеристики безопасности представлен на рис.8.

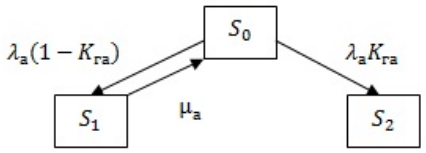


Рис.8. Граф системы состояний случайного процесса для угрозы атаки с фатальным отказом для укрупненной марковской модели

Применение укрупненной марковской модели угрозы атаки как системы с отказами, восстановлениями и фатальным отказом существенно упрощает задачу проектирования системы защиты информационной системы в том случае, когда на момент проектирования системы защиты для используемых в информационной системе средств (например, операционной системы и используемых приложений) уже были построены укрупненные

марковские модели угрозы атаки как системы с отказами и восстановлениями характеристики безопасности, т.е. определены соответствующие характеристики потенциально возможных для информационной системы угроз атак: интенсивности возникновения λ_a и интенсивности устранения μ_a реальных угроз атак.

Как ранее отмечали, информационная безопасность имеет несколько ключевых характеристик, к которым относятся: конфиденциальность, целостность и доступность обрабатываемой информации. Если система с фатальным отказом в отношении нарушения конфиденциальности информации может рассматриваться как невосстанавливаемая, то в отношении нарушения целостности и доступности информации можно говорить о восстанавливаемом фатальном отказе. Восстановление осуществляться с некоторой интенсивностью $\mu_в$ (в первом случае восстанавливается доступность обрабатываемой информации, например, это может потребовать переустановки системных средств или приложений и т.д., во втором случае – собственно данные, например, из резервной копии). При моделировании подобной системы важно оценить вероятность появления восстанавливаемого фатального отказаза счет реализации угрозы атаки и среднее время наработки системы на подобный отказ; среднее время восстановления системы $1/\mu_в$ может быть оценено с использованием соответствующей статистики. Отметим, что параметр $\mu_в$ никак не связан с устранением выявленных в системе уязвимостей – это интенсивность восстановления, соответственно, системы или информации.

Для получения требуемых характеристик в укрупненную марковскую модель угрозы атаки как системы с отказами, восстановлениями и фатальным отказом, граф системы состояний которой приведен на рис.8, следует включить переход из состояния S_2 (S_2 уже становится непоглощающим состоянием) в состояние S_0 с интенсивностью $\mu_в$.

Используя данную модель можно рассчитать вероятность P_2(как относительную долю времени) нахождения системы в состоянии S_2, характеризуемом соответственно нарушением доступности или целостности информации, интенсивность потока возникновения подобных фатальных отказов $\lambda_{фо}$:

$$\lambda_{фо} = \omega = P_0 K_{га} \lambda_а,$$

и среднее время наработки системы на восстанавливаемый фатальный отказ, определяемое как $1/\lambda_{фо}$.

Ключевым вопросом возможности и обоснованности практического применения приведенных выше моделей угрозы атаки с фатальным отказом является возможность и обоснованность задания характеристики $K_{га}$ – вероятности (коэффициента готовности) осуществить атаку (реализовать угрозу атаки) потенциальным нарушителем (реализовать

создавшуюся в информационной системе реальную угрозу атаки). При этом значение $K_{га}$ должно задаваться количественно, причем коэффициент $K_{га}$ должен быть универсальным для разнородных угроз атак. Естественно, что коэффициент $K_{га}$ должен определяться применительно к конкретной информационной системе, обрабатывающей конкретную информацию, которой в конечном счете и определяется заинтересованность и возможность нарушителя в реализации угрозы атаки той или иной сложности. Данная задача решается путем построения математической модели нарушителя – потенциального нарушителя безопасности конкретной информационной системы.

1.4. Математическая модель потенциального нарушителя. Определение вероятности (коэффициента готовности)реализовать угрозу атаки потенциальным нарушителем

Риск реализации атаки на информационную систему невозможно оценить без построения модели потенциального нарушителя безопасности, без подобной оценки можно оценить лишь риск отказа безопасности информационной системы – возникновения реальной угрозы атаки. Естественно, что данной моделью должны учитываться заинтересованность злоумышленника в реализации атаки на конкретную информационную систему и его потенциальные возможности (очевидно, что эти характеристики взаимосвязаны).

Отметим, что построение модели нарушителя является ключевым вопросом при моделировании характеристик безопасности информационных систем. Без возможности количественного задания коэффициента $K_{га}$ расчет характеристик безопасности конкретной информационной системы, для которой проектируется система защиты, невозможен, см. рис.7 и рис.8.

В настоящее время модель потенциального нарушителя безопасности формируется как набор предположений о возможном нарушителе безопасности, его квалификации, технических и материальных возможностях и т.д. При этом строится неформальная модель нарушителя, отражающая причины и мотивы действий, априорные знания, преследуемые цели, их приоритетность для нарушителя, основные пути достижения поставленных целей: способы реализации исходящих от него угроз, место и характер действия, возможная тактика и т.п. В конечном счете подобная модель используется с целью выявления совокупности актуальных угроз атак для конкретной информационной системы, для которой проектируется система защиты информации, именно актуальных, поскольку потенциально возможные угрозы атак определяются возможностью их технической реализации на информационную систему (архитектура, используемые программные и аппаратные средства и т.д.).

Математическое же моделирование нарушителя сводится к моделированию воздействия нарушителя на защищаемую систему и представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, характеризующих результаты действий и функциональных (аналитических, численных или алгоритмических) зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами защищаемого объекта [4].

Однако подобный подход к моделированию не позволяет количественно оценить актуальность угрозы атак, учесть эту важнейшую характеристику безопасности при проектировании системы защиты для конкретной информационной системы.

Модель нарушителя должна учитывать достаточно много факторов, не все из которых поддаются формализованному описанию. Это, прежде всего, уровень заинтересованности в получении несанкционированного доступа к конкретной информации, это уровень квалификации нарушителя, позволяющий ему осуществить ту или иную атаку, его информированность о выявлении и устранении различно рода уязвимостей, наличие соответствующих инструментальных средств для осуществления атаки, информированность о реализованных в конкретной информационной системе технологиях (возможность получения подобной информации), в том числе технологиях защиты информации, используемом программном обеспечении, регламентах и другое. Сложность учета всех этих (итак трудно формализуемых) факторов обусловливается не только их количеством и разнородностью, но и сложностью формализации каких-либо зависимостей между ними (например, нарушитель может нанять высококвалифицированного специалиста для осуществления атаки, может приобрести соответствующие автоматизированные средства осуществления атаки – реализовать сложную атаку, не обладая при этом должной квалификацией, и т.д.). Вместе с тем, нам необходима некая интегральная оценка, причем количественная, позволяющая учесть все эти факторы, иначе невозможно приступить к проектированию системы защиты для конкретной информационной системы. Крайне важным является и следующий момент. Атаки разнородны по своей природе (локальные, сетевые, предполагающие внедрение вредоносной программы, использование ошибки в приложении, в системном драйвере и многое другое). Как следствие, необходим такой подход к оцениванию, который бы позволил ввести некую единую шкалу оценки актуальности угроз атак вне зависимости от их природы.

Задумаемся над следующим. В чем, в конце концов, находят свое отражение все эти разнородные факторы? Ответ на этот вопрос оказывается достаточно прост: в сложности реализуемых нарушителем атак на конкретную информационную систему (сложность реализуемых нарушителем атак зависит и от заинтересованности, и от квалификации, и от технических возможностей нарушителя, от его информированности об информационной

системе и т.д.). Говоря же о конкретной информационной системе, подразумеваем, что речь идет об информационной системе, обрабатывающей определенную конкретную (содержание, объем) информацию, поскольку именно к обрабатываемой информации злоумышленником и осуществляется несанкционированный доступ. Развивая эту мысль, введем понятие подобной информационной системы, под которой будем понимать систему, обрабатывающую подобную (содержание, объем), в идеале для проектирования аналогичную информацию. Отметим, что в той или иной мере подобная система при проектировании системы защиты конкретной информационной системы может быть определена (всегда с той или иной достоверностью можно найти некий аналог).

Исходя из того, что нарушитель информационной системы может быть охарактеризован сложностью реализуемых им атак на эту систему, определимся с тем, как количественно оценить сложность атаки (сложность реализации угрозы атаки): введем количественную меру сложности атаки (сложности реализации угрозы атаки), поскольку в общем случае следует говорить о том, готов ли (заинтересован ли и может ли) нарушитель реализовать атаку определенной сложности. При этом,как отмечали,иугрозы уязвимостей, создающие угрозу атаки, и собственно угрозы атаки по своей сути разнородны, количественная же мера должна быть единой.

Обратимся к основам теории информации, понимая, что для осуществления успешной атаки на отдельно взятую уязвимость нарушитель должен обладать соответствующей информацией в отношении угрозы этой уязвимости – информацией о том, что такая уязвимость выявлена и не устранена, т.е. неким количеством информации в отношении угрозы уязвимости. Т.к. нас интересует исключительно вероятность того, что уязвимость присутствует в информационной системе– угроза уязвимости реальна, при этом возможны два исхода события: уязвимость присутствует либо нет, количество информации в отношении уязвимости в данном случае следует рассматривать как вероятностную меру.

Замечание. Сложность технической реализации атак на те уязвимости, которые требуют разработки соответствующих программных средств (эксплоитов) для их эксплуатации при реализации атаки, как отмечалось ранее, учитывается при задании соответствующего параметра уязвимости – интенсивности возникновения угрозы уязвимости λ. При задании этого параметра на основании анализа соответствующей статистики уязвимостей должна рассматриваться только та часть уязвимостей, для которых за анализируемый период времени подобные эксплоиты были разработаны и использованы.

Вероятностная мера количества информации I(в рассматриваемом случае – в одном сообщении) определяется по формуле [20]:

$$I = -log_2 P_i,$$

гдеP_i – вероятность i -го исхода.

В нашем случае неопределенность можно рассматривать в отношении любой угрозы уязвимости, которая может использоваться нарушителем при осуществлении атаки, вероятность присутствия которой (реальная угроза) в системе определяется как $1 - P_{0\text{у}}$. Нарушитель для осуществления успешной атаки должен обладать соответствующей информацией в отношении присутствия уязвимости в системе, т.е. получить сведения, уменьшающие неопределенность в отношении данной угрозы уязвимости. Очевидно, что чем выше для угрозы уязвимости значение $P_{0\text{у}}$ (в общем случае уязвимость реже возникает и за меньшее время устраняется), тем сложнее нарушителю осуществить соответствующую атаку.

С учетом сказанного сложность реализацииугрозы уязвимости (обозначим ее $S_{\text{у}}$) может интерпретироваться как вероятностная мера количества информации$I(P_{0\text{у}})$, которым должен обладать злоумышленник для реализации этой угрозы, как следствие, может быть определена следующим образом [23]:

$$S_{\text{у}} = I(P_{0\text{у}}) = -log_2(1 - P_{0\text{у}})$$

Корректность использования данной метрики для оценки реализации угрозы уязвимости обосновывается использованием логарифмической функции (в нашем случае по основанию 2, поскольку у события возможны два исхода), позволяющей соответствующим образом учесть нелинейность функции изменения сложности реализации нарушителем угрозы уязвимости от изменения значения вероятности $P_{0\text{у}}$: $S_{\text{у}} = f(P_{0\text{у}})$.

Проиллюстрируем сказанное примером, для чего сравним сложностиреализации двух угроз уязвимостей, пусть для одной из них значение характеристики $P_{0\text{у}}$составляет 0,7, а для другой – 0,99. Видим, что в первом случае$S_{\text{у}1} = 1{,}74$, во втором случае $S_{\text{у}2} = 6{,}64$, т.е. реализация угрозы второйуязвимости для нарушителя в 3,82 раза сложнее, чем реализация первой угрозы уязвимости (ему понадобится в 3,82 раза больше количества информации об угрозе уязвимости с целью снятия неопределенности в отношении наличия в системе этой уязвимости – создания в системе реальной угрозы).

Замечание. Единица сложности реализации угрозы уязвимости$S_{\text{у}} = I(P_{0\text{у}}) = 1$ задается условием $P_{0\text{у}} = 0{,}5$, определяющим то, что уязвимость с равной вероятностью присутствует в системе (реальная угроза) либо нет.

Поскольку угрозу атаки создает соответствующая совокупность выявленных и не устраненных в системе уязвимостей (реальных угроз уязвимостей), сложность атаки для нарушителя в общем случае определяется совокупной сложностью атак на каждую создающую угрозу атаки угрозу уязвимости. Если рассмотреть атаку как последовательность использования нарушителем выявленных и не устраненных в системе уязвимостей, имеющих характеристики

P_{0yr} и S_{yr}, $r=1,\ldots,R$, можно ввести количественную характеристику сложности атаки $I(P_{0a})$ (обозначим ее S_a), где $S_a = I(P_{0a})$, которая определяется количеством информации, которым должен обладать нарушитель для осуществления успешной атаки, угрозу которой создают R выявленных в системе и не устраненных уязвимостей (с учетом того, что события возникновения (выявления)реальных угроз уязвимостей являются независимыми, а условием реализации нарушителем угрозы атаки является наличие в системе одновременно всех уязвимостей, создающих угрозу атаки):

$$S_a = I(P_{0a}) = -log_2(1 - P_{0a}) = -log_2 \prod_{r=1}^{R}(1 - P_{0yr}),$$

где

$$P_{0a} = 1 - \prod_{r=1}^{R}(1 - P_{0yr})$$

– вероятность того, что в любой момент времени угроза атаки реальна.

Используя же соответствующее свойство логарифмов, можем записать:

$$S_a = I(P_{0a}) = \sum_{r=1}^{R} I(P_{0yr}) = \sum_{r=1}^{R} S_{yr}$$

При этом информация, получаемая нарушителем, рассматривается с точки зрения ее полезности (ценности) для достижения потребителем информации поставленной практической цели – в нашем случае для осуществления нарушителем успешной атаки на информационную систему.

Замечание. Использование в информационной системе системы защитыувеличивает значение сложности реализации соответствующей угрозы атаки на информационную систему на величину сложности реализации угрозы атаки на систему защиты информации.

Отметим, что характеристика ΔS_a может рассматриваться в качестве так называемой в теории информации прагматической меры количества информации, определяемой в данном случае по формуле:

$$\Delta S_a = log_2(1 - P_{0a\text{исх}}) - log_2(1 - P_{0\text{азащ}}) = log_2 \frac{(1-P_{0a\text{исх}})}{(1-P_{0\text{азащ}})},$$

где $P_{0a\text{исх}}$ *и* $P_{0\text{азащ}}$ – вероятности готовности к безопасной эксплуатации исходной и защищенной (при использовании системы защиты) информационных систем.

Прагматика данной оценки состоит в выявлении условий, при которых необходима реализация соответствующих мер защиты для информационной системы.

Универсальность данной метрики обусловливается тем, что она позволяет сравнивать между собою сложности реализации разнородных атак, основанных на различных принципах реализации, в общем случае использующих совершенно различные по своей природе угрозы уязвимостей.

Как отмечалось, коэффициент готовности нарушителя осуществить атаку $K_{\text{га}}$ требуется определять применительно к конкретной информационной системе при проектировании для нее системы защиты. На практике при решении задачи проектирования может рассматриваться (и, как правило, рассматривается) некая подобная информационная система (аналог), характеризуемая обработкой аналогичной информации, что и определяет заинтересованность и возможности нарушителя. В отношении аналога, как правило, существует соответствующая статистика реализованных (в том числе и отраженных) на информационную систему атак в процессе ее эксплуатации.

С учетом сказанного математическая модель нарушителя (количественная интегральная оценка заинтересованности и возможности реализации злоумышленником атаки на конкретную информационную систему) может быть представлена следующим образом[23]:

$$S_{a\text{н}} = \max\{S_{a\text{н}m}, m = 1, \dots, M\},$$

где $S_{a\text{н}}$ – максимальная сложность реализованных (с учетом и отраженных) в подобной информационной системе атак, характеризуемых $P_{0a\text{н}}$, определяемая на множестве выявленных совершенных атак на подобную информационную систему (аналог) в процессе ее эксплуатации $S_{a\text{н}m}, m = 1, \dots, M$.

Имея значение характеристики$S_{\text{а}}$ – характеристика сложности реализации какой-либо угрозы атаки на информационную систему, для которой проектируется система защиты, и значение характеристики$S_{a\text{н}}$– характеристика максимальной сложности реализованных (в том числе и отраженных) в подобной информационной системе атак, можно определить искомую характеристику коэффициента готовности (или вероятности) нарушителя осуществить атаку сложности$S_{\text{а}}$на конкретную информационную систему (для которой проектируется система защиты) $K_{\text{га}}$:

$$K_{\text{га}} = \begin{cases} \dfrac{S_{a\text{н}}}{S_a}, \text{если } S_{a\text{н}} < S_a \\ 1, \text{если } S_{a\text{н}} \geq S_a \end{cases}$$

Исходя же из того, что

$$K_{\text{га}} = \frac{S_{a\text{н}}}{S_a} = \frac{log_2(1-P_{0a\text{н}})}{log_2(1-P_{0a})} = log_{1-P_{0a}}(1 - P_{0a\text{н}}),$$

коэффициент$K_{\text{га}}$может интерпретироваться как значение степени, в которую надо возвести значение вероятности осуществления атаки на информационную систему $(1 - P_{0a})$, для получения значения вероятности атаки, которую может успешно реализовать нарушитель$(1 - P_{0a\text{н}})$.

Как видим, для расчета значений искомой характеристики не требуется использования каких-либо экспертных оценок.При рассмотренном подходе к моделированию опять же используются только стохастические параметры угроз уязвимостей и статистика в отношении

безопасности эксплуатации аналогичных систем при проектировании системы защиты конкретной информационной системы.

С использованием введенного коэффициента готовности злоумышленника осуществить успешную атаку сложностиS_a на информационную систему $К_{га}$ (нарушитель готов осуществить подобную атаку – характеристика нарушителя, которая может рассматриваться как вероятность реализации нарушителем успешной атаки при условии неготовности информационной системы к безопасной эксплуатации в отношении атаки, что определяется условиемP_{0a}=0), с учетом того, что информационная система готова к безопасной эксплуатации в отношении угрозы атаки задается характеристикой P_{0a} (характеристика безопасности в отношении угрозы атаки), формула для расчета вероятности реализации в любой момент времени успешной атаки на информационную системуP_a имеет следующий вид:

$$P_a = K_{га} \prod_{r=1}^{R} (1 - P_{0уr})$$

Естественно, вероятность того, что успешная атака не будет осуществлена на информационную систему, определяется как $P_{0а}$:

$$P_{0a} = 1 - K_{га} \prod_{r=1}^{R} (1 - P_{0уr})$$

1.5. Моделирование угрозы атаки с использованием аппроксимирующей функции

На практике при решении задачи проектирования системы защиты, в том числе для формирования требований к характеристикам безопасности защищенной информационной системы, включая учет реальных и потенциальных рисков [13,19] для оценки экономической целесообразности применения той или иной системы защиты, крайне важна оценка изменения вероятности отказа характеристики безопасности (соответственно, готовности к безопасной эксплуатации) в процессе эксплуатации информационной системы.Проиллюстрируем сказанное.

Пусть потери от несанкционированного доступа к информации (в результате ее хищения либо удаления или модификации) составляют $C_{инф}$. Тогда риск потерь применительно к угрозе безопасности информационной системы в целом (характеристика угрозы безопасности информационной системы P_{0a}) можно оценить следующим образом[13]:

$$R_{C_{Уинф}} = C_{инф} (1 - P_{0a})$$

Если использовать при проектировании системы защиты соответствующую марковскую модель, полученную ранее, то, определив среднее время наработки информационной системы до реализации на нее успешной атаки, определяем тем самым средний интервал времени

эксплуатации системы, через который потери составят $C_{\text{инф}}$. Данный подход к моделированию не дает возможности ответить на вопрос: а каков будет риск потерь на некотором интервале времени эксплуатации системы меньшем среднего времени наработки информационной системы до реализации на нее успешной атаки и как риск потерь распределен во времени эксплуатации системы[22]? Важность подобной оценки обусловливается тем, что кроме потенциальных потерь, связанных с несанкционированным доступом к обрабатываемой информации, при внедрении системы защиты присутствуют еще и реальные потери, определяемые стоимостью внедряемой системы защиты $C_{сзи}$ и удельной стоимостью (стоимостью в единицу времени) ее эксплуатации $C_{уэсзи}(t)$.Заметим, что в первом приближении можно рассматривать линейную зависимость изменения стоимости эксплуатации системы защиты во времени.При этом возникает оптимизационная задача задания требуемого значения характеристики защищаемой информационной системы $P_{0\text{у}}$ при проектировании системы защиты с учетом того, что потенциальные потери от несанкционированного доступа к обрабатываемой информации при условии $t \longrightarrow \infty$ стремятся к $C_{\text{инф}}$, в то время как потери, связанные с эксплуатацией системы защиты при тех же условиях стремятся к ∞ (т.е. задание значения $P_{0\text{у}}$ из условия «чем больше, тем лучше», естественно менее единицы, в общем случае с учетом сказанного некорректно).

Задача моделирования состоит в следующем. Как ранее отмечали, в процессе эксплуатации информационной системы реальная угроза атаки средней продолжительностью $1/\mu_{уа}$, в случае если она не будет реализовываться нарушителем, в среднем через интервалы времени $T_{0\text{уа}}$ будет многократно возникать (характеристика $T_{0\text{уа}}$определяется с использованием укрупненной марковской модели угрозы атаки как системы с отказами и восстановлениями характеристики безопасности). При этом каждую возникающую реальную угрозу атаки нарушитель может использовать, реализовав атаку, с вероятностью $K_{га}$. Иллюстрация сказанного приведена на рис.9.

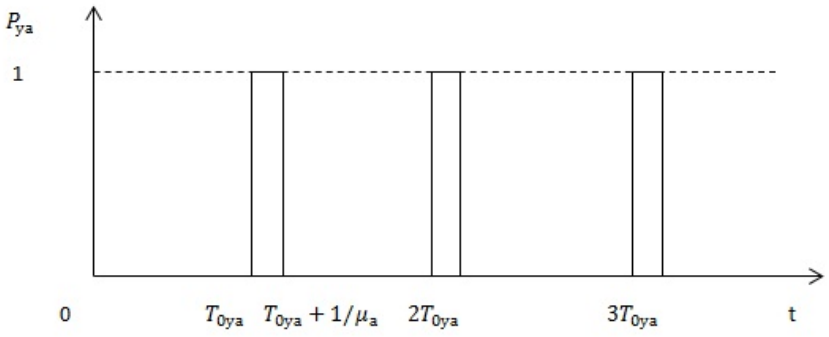


Рис.9. Иллюстрация появления реальной угрозы атаки в процессе эксплуатацииинформационной системы

Рассчитать значение характеристики P_{ya}, достигаемое при эксплуатации системы в некоторый момент времени t, кратный T_{0ya}, при условии $t \geq T_{0ya}$, обозначим $P_{ya}(t \geq T_{0ya})$, можно следующим образом [22]:

$$P_{ya}(t \geq T_{0ya}) = \sum_{i=1}^{\lfloor t/T_{0ya} \rceil} K_{га}(1 - K_{га})^{i-1},$$

где через $\rfloor d \lceil$ обозначено меньшее целое числа d.

Изменение характеристики P_{ya} во времени проиллюстрировано на рис.10.

Рис.10. Иллюстрация изменения характеристики $P_{уа}(t \geq T_{0уа})$в процессе эксплуатациииинформационной системы

Для расчета значения $P_{уа}(t \geq T_{0уа})$ в любой момент времени tэксплуатации информационной системыможнопостроить и использовать соответствующую аппроксимирующую функцию. Основное правило аппроксимации при этом состоит в том, что значение аппроксимирующей функции, обозначим ее$P_{Ауа}(t)$, для любого момента времени $iT_{0уа}$ должно быть не меньше значения функции $P_{уа}(t \geq T_{0уа})$ в соответствующий момент времени – аппроксимирующая функция должна предоставлять возможность получения соответствующей граничной оценки, что требуется при проектировании системы защиты, см. рис.11.

Рис.11. Иллюстрация требований к аппроксимирующей функции $P_{Ауа}(t)$

Таким образом, с использованием построенной подобным образом аппроксимирующей функции в отношении угрозы атаки можно определить вероятность возникновения реальной угрозы атаки $P_{уа}$на конкретную информационную систему с учетом готовности реализации этой атаки нарушителем в любой момент времени t эксплуатации информационной системы – вероятность фатального отказа $P_{\text{Ауа}}(t)$, как следствие, и величину потенциальных потерь $R_{C_{\text{Уинф}}}(t)$:

$$R_{C_{\text{Уинф}}}(t) = C_{инф} P_{\text{Ауа}}(t)$$

В общем случае искомая аппроксимирующая функция имеет следующий вид:

$$P_{\text{Ауа}}(t) = (((1/(1-K_{\text{га}}))^{t/T_{\text{0уа}}} - 1)(1-K_{\text{га}})^{t/T_{\text{0уа}}}$$

Рассмотрим некоторое пороговое значение времени эксплуатации защищенной информационной системы $\text{Т}_{\text{0Узиспор}}$, для которого могут быть определены реальные потери, связанные с внедрением и эксплуатацией системы защиты информации, из условия:

$$C_{\text{инф}} P_{Ауа}(\text{Т}_{\text{0Узиспор}}) = C_{\text{сзи}} + \text{Т}_{\text{0Узиспор}} C_{\text{уэсзи}}(t).$$

Очевидно, что требование к продолжительности безопасной эксплуатации защищенной информационной системы, превышающее значение характеристики $\text{Т}_{\text{0Узиспор}}$, не имеет смысла, поскольку в данном случае реальные потери, связанные с внедрением и эксплуатацией системы защиты информационной системы, превысят потенциальные потери, связанные с возможностью несанкционированного доступа к обрабатываемой информации.

1.6. Интерпретация и марковскиемодели угрозы безопасности информационной системы

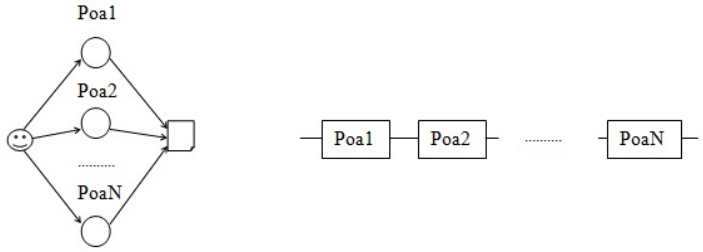
1. Интерпретация угрозы безопасности информационной системы.

Угроза безопасности информационной системы (информационной системы в целом) также может быть представлена соответствующим орграфом [23]. При этом угроза безопасности информационной системы уже может интерпретироваться (может быть представлена) схемой последовательного резервирования, резервируемыми и резервирующими элементами которой являются угрозы атак.

Замечание. Как ранее отмечали, информационная безопасность имеет несколько ключевых характеристик, к которым относятся: конфиденциальность, целостность и доступность обрабатываемой информации [1]. Говоря об угрозе безопасности информационной системы и о создаваемых ее угрозах атак, естественно, подразумеваем угрозу нарушения одной из данных характеристик безопасности, поскольку потенциальные угрозы атак, направленных на нарушение конфиденциальности, целостности и доступности обрабатываемой информации, в общем случае могут сильно различаться.

Используем обозначениеP_{0ym}– вероятности того, что информационная система готова к безопасной эксплуатации в отношении *m*-й угрозы уязвимости, *m=1,...,M*(соответствующие наборы уязвимостей создают угрозы атак), а P_{0an} – вероятности того, что информационная система готова к безопасной эксплуатации в отношении *n*-й угрозы атаки, *n=1,...,N*. Вероятность того, что информационная система готова к безопасной эксплуатации, обозначим через P_{0y}.

Угроза безопасности информационной системы может интерпретироваться схемой последовательного резервирования угроз атак,резервируемыми и резервирующими элементами которой являются угрозы атак, см. рис.12, поскольку каждая угроза атаки, присутствующая в системе с вероятностью $1 - P_{0an}$, создает угрозу безопасностиинформационной системы в целом[23].

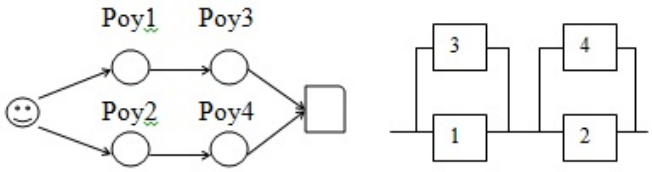


а. Оргграф угрозы безопасности информационной системы

б. Схема последовательного резервирования

Рис.12. Оргграф угрозы безопасности информационной системы и ее интерпретация схемой последовательного резервирования угроз атак

Соответственно в общем случае угроза безопасности информационной системы может интерпретироваться схемой последовательно-параллельного резервирования угроз уязвимостей. В примере орграфа угрозы безопасности информационной системы, приведенном на рис.13.а, первая уязвимость резервируется третьей, вторая – четвертой. С учетом этого может быть получена схема резервирования, приведенная на рис.13.б.

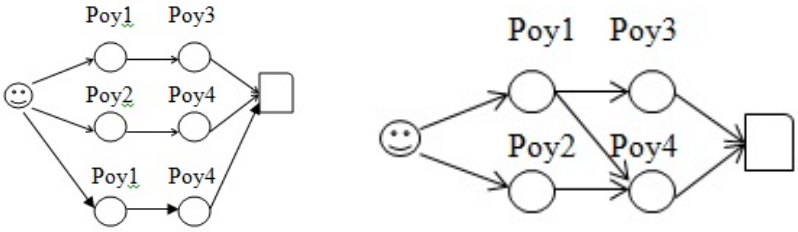


а. Оргграф

б. Схема резервирования

Рис.13. Пример орграфа безопасности информационной системы и ее интерпретация схемой последовательно-параллельногорезервирования угроз уязвимостей

Приведем пример орграфа угрозы безопасности информационной системы, в котором угрозы атак зависимы по угрозам уязвимостей, в качестве элементов (вершин) которого будем рассматривать угрозы уязвимостей (пусть информационная система подвержена трем угрозам атак, создаваемых соответствующими угрозами уязвимостей), см. рис.14.а.



а. Исходный орграф б. Приведенный орграф

Рис.14. Иллюстрация приведения орграфа угрозы безопасности информационной системы

Рис.14 иллюстрирует зависимость угроз атак по угрозам уязвимостей (на рис.14 это первая и четвертая уязвимости).Это обусловливает возможность построить для исходного орграфа, см. рис.14.а, приведенный орграф угрозы безопасности информационной системы, см. рис.14.б, в котором угроза каждой уязвимости встречается только один раз.

Замечание. При проектировании системы защиты информационной системы взвешенные вершины проектируемой системы защиты уже соответственнос параметрами системы защиты $\lambda_{\text{сзи}}$ и $\mu_{\text{сзи}}$, характеризующими угрозы уязвимостей собственно системы защиты, включаются в соответствующие орграфы угроз атак и угрозы безопасности информационной системы, поскольку для реализации атаки на защищенную информационную систему необходимо использовать не только уязвимости информационной системы, но и уязвимости системы защиты.

Вернемся к количественной оценке актуальности угрозы уязвимости, но уже применительно к информационной системе в целом. Ранее мы сделали два, по сути, противоречащих друг другу вывода в отношении количественной оценки актуальности угрозы уязвимости. Моделируя угрозу уязвимости, мы сделали вывод о том, что более актуальна для нивелирования та угроза уязвимости, которая характеризуется меньшим значением характеристики $P_{0\text{у}}$. Естественно, в данных предположениях в первую очередь нивелировать системой защиты следует более актуальную в этом смысле уязвимость. Однако, моделируя угрозу атаки, мы сделали вывод о том, что не важно, какую из угроз уязвимости, используемых атакой, следует нивелировать системой защиты, важны лишь параметры безопасности собственносистемы защиты. Возникает вопрос: как все-таки количественно оценить актуальность угрозы уязвимости?Это ключевой вопрос при разработке метода проектирования системы защиты, определяющий критерий оптимальности – критерий выбора актуальной

угрозы уязвимости для нивелирования системой защиты (без определения данного критерия невозможно перейти к вопросам проектирования).

Предположим, что в орграфе угрозы безопасности информационной системы представлены только актуальные для информационной системы угрозы атак, т.е. в отношении всех этих атак должна быть реализована соответствующая защита. Обратимся к приведенному орграфу, представленному на рис.14.б. Если системой защиты нивелируется третья угроза уязвимости, то ею будет реализована защита от одной актуальной угрозы атаки, использующей 1 и 3 угрозы уязвимости; если же системой защиты нивелировать угрозу первой уязвимости, то ею будет реализована защита сразу от двух угроз атак: от атаки, использующей угрозы 1 и 3 уязвимостей, и от атаки, использующейугрозы 1 и 4 уязвимостей. Очевидно, что с точки зрения оптимизации системы защиты информации (оптимизации набора решаемых ею задач защиты информации), в данном примере более актуально нивелирование угрозы первой уязвимости.

С учетом сказанного введем соответствующую количественную меру актуальности угрозы уязвимости в информационной системе [23].

Количественной мерой актуальности угрозы уязвимости в информационной системе является то, каким количеством актуальных угроз атак на информационную систему используется эта уязвимость, соответственно, от какого количества угроз атак защищается информационная система при нивелировании системой защиты данной угрозы уязвимости. Таким образом, актуальность угрозы уязвимости для информационной системы количественно можно оценить с использованием коэффициента актуальности угрозы уязвимости k[23]:

$$k = US,$$

где U– число актуальных угроз атак, входящих в вершину угрозы уязвимости на орграфе, S– число актуальных угроз атак, исходящих из вершины угрозы уязвимости на орграфеугрозы безопасности информационной системы. При этом чем больше для угрозы уязвимости значение коэффициента k, тем актуальнее угроза данной уязвимости для нивелирования ее системой защиты в информационной системе.

Данный подход к количественному оцениванию актуальности угрозы уязвимости, полученный на основании рассмотренной интерпретации угрозы безопасности информационной системы, положен в основу метода формального проектирования системы защиты информационной системы, применяемого для определения оптимального набора задач защиты, решаемых проектируемой для какой-либо конкретной информационной системы системой защиты, который будет рассмотрен в следующем разделе.

2. Марковская модель угрозы безопасности информационной системы как системы с отказами и восстановлениями характеристики безопасности.

Рассмотрим математическое описание марковского процесса с дискретными состояниями и непрерывным временемдлявграфа угрозы безопасности информационной системы, создаваемой угрозами двух атак: первая из которых создается угрозами первой и второй уязвимостей, вторая – угрозами первой и третьей уязвимостей (рассматриваем зависимые угрозы атак по угрозам уязвимостей). В качестве состояний графапереходов рассматриваются состояния возникновения и устранения именно угроз уязвимостей. Корректность такого подхода к моделированию угрозы безопасности информационной системы обусловливается тем, что угрозы атак зависимы по угрозам уязвимостей, как следствие, рассмотрение на графе переходов в качестве состояний возникновения и устранения угроз атак в данном случае некорректно, что обоснуем далее.

Замечание.Для того чтобы не приводить громоздких рисунков исследования, проводим на достаточно простом примере угрозы безопасности информационной системы (понятно, что все получаемые здесь и далее результаты применимы при моделировании угрозы безопасности информационной системы любой сложности), при этом для проведения необходимых исследований рассматриваем случай с зависимостью угроз атак по уязвимостям.

Граф системы состояний случайного процесса для рассматриваемой системы представлен на рис.15.

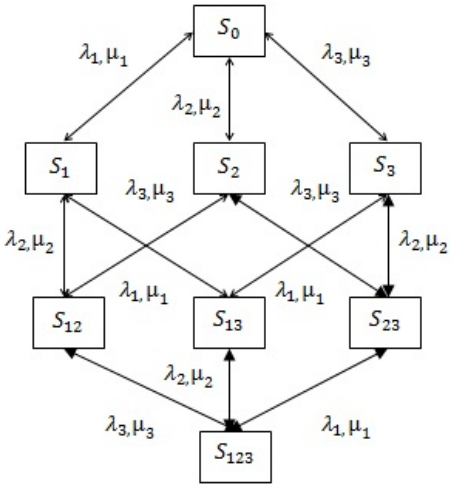


Рис.15. Граф системы состояний случайного процессадля угрозы безопасности информационной системы

На графе представлены следующие возможные состояния: S_0 – исходное состояние системы, S_i – в системе выявленаи не устранена одна из уязвимостей, S_{ij} – в системе выявлены и не устранена две уязвимости, S_{ijl} – в системе выявлены и не устранены все три уязвимости. Предполагаем, что все переходы системы из одного состояния в другое происходят под воздействием простейших потоков событий с соответствующими интенсивностями возникновения λ_i или устранения μ_i реальных угроз уязвимостей, а вероятность

одномоментного выявления, равно как устранения нескольких уязвимостей, пренебрежимо мала.Переходы системы в состояния S_{12} и в S_{13} связаны с появлением в системе реальных угроз соответствующих атак (возникает реальная угроза безопасности информационной системы). Переходы системы в состояние S_{123} также связаны с возникновением реальной угрозы безопасности информационной системы, для этого состояния характерной возникновения реальных угроз обеих атак. Переход же из состояния S_{23} в состояние S_{123} как раз и характеризует одномоментное возникновение в системе обеих угроз атак (при возникновении первой угрозы уязвимости при наличии второй и третьей), что, как видим, учитывается при данном способе моделирования.

А теперь предположим, что в качестве элемента безопасности рассматривается угроза атаки. В данном случае имеем две угрозы атаки, марковкая модель будет описываться графом, представленным на рис.6.а, с той разницей, что в качестве интенсивностей переходов будут использоваться параметры угроз атак. Сравним данный граф с графом, представленным на рис.15. Как видим, принципиальное отличие заключается в наличии состояния S_{23}; напомним, что переход из состояния S_{23} в состояние S_{123} характеризует одномоментное возникновение в системе обеих угроз атак. Подобное событие (состояние) моделью, описываемой графом, представленным на рис.6.а, где в качестве интенсивностей переходов используются параметры угроз атак, учесть априори невозможно, поскольку любая марковская модель строится в предположении, что одномоментно в системе два события не происходят (из любого состояния возможен переход только в одно состояние).С учетом сказанного можно сделать крайне важный вывод.

Вывод.

Рассматривая в качестве элемента безопасности угрозу атаки, невозможно построить корректную марковскую модель угрозы безопасности информационной системы при зависимости угроз атак по угрозам уязвимостей, что, как правило, и имеет место на практике.

Замечание. В случае же, если рассматривать в качестве элемента безопасности угрозу уязвимости, при зависимости угроз атак по угрозам уязвимостей получаем корректную марковскую модель угрозы безопасности информационной системы, что иллюстрирует граф, представленный на рис.15.

Отметим, что при подобном подходе к моделированию для исходного и для приведенного орграфов угрозы безопасности информационной системы строится один и тот же граф системы состояний случайного процесса (граф переходов), что легко объяснимо, поскольку данные орграфы содержат один и тот же набор вершин и переходов между вершинами.

Другой важный вывод, который можно сделать, анализируя представленный граф, состоит в том, что на характеристики безопасности информационной системы никак не сказывается порядок использования нарушителем угроз уязвимостей при осуществлении атаки. Важен исключительно состав угрозы атаки (набор создающих ее угроз уязвимостей), т.е. угрозы атак, создаваемых одними и теми же угрозами уязвимостей, эквиваленты вне зависимости от порядка использования угроз уязвимостей при осуществлении атаки. Как следствие, различные угрозы атак, характеризуемые одним набором создающих их угроз уязвимостей, могут рассматриваться как одна и та же угроза атаки.

Используя данную модель по аналогии с тем, как это может быть сделано применительно к определению соответствующей характеристики безопасности для угрозы атаки, может быть определенавероятность готовности информационной системы к безопасной эксплуатации $P_{0у}$(или стационарный коэффициент готовности системы $К_{гс}$), который для графа, приведенного на рис.15, определяется следующим образом:

$$К_{гс} = P_{0у} = P_0 + P_1 + P_2 + P_3 + P_{23}$$

Замечание. Построение укрупненной модели угрозы безопасности информационной системы как системы с отказами и восстановлениями характеристики безопасности некорректно ввиду зависимости угроз атак по угрозам уязвимостей. На рис.15 это иллюстрирует наличие состояния S_{23}.

3. Марковская модель угрозы безопасности информационной системы как системы с отказами, восстановлениями и фатальным отказом характеристики безопасности.

Прежде всего, рассмотрим особенности оценивания вероятности фатального отказа характеристики безопасности в информационной системе с целью определения в конечном счете того, каким образом задать на марковской модели интенсивности переходов в состояние (поглощающее состояние), соответствующее фатальному отказу. Важным в данном случае является то, что сколько бы не было одновременно создано в информационной системе реальных угроз атак (под реальной понимаем угрозу атаки, созданную выявленными и не устраненными уязвимостями, т.е. характеризуемую условием $P_{0an} = 0$), которые могут быть реализованы нарушителем,им в любой момент времени будет реализована только одна из них, и этого достаточно для нарушения характеристики безопасности (что полностью соответствует представленной интерпретации угрозы безопасности информационной системы схемой последовательного резервирования угроз атак), т.к. будет осуществлен несанкционированный доступ к обрабатываемой информации, а это фатальный отказ характеристики безопасности. Как следствие, вероятностью реализации в системе нарушителем одновременно двух и более атак можно пренебречь.

Исходя из того, что с вероятностью $(1–P_{0an})$, $n = 1,…,N$, в системе появится n-я реальная угроза атаки, для вероятности перехода системы из безопасного состоянияS_0, в котором она находится с вероятностью $P_{0У}$, в одно из состояний фатального отказа безопасностиS_n, $n = 1,…,N$ (число состояний системы здесь будет равно n+1, а не 2^n)по причине реализации соответствующей атаки нарушителем, характеризуемого P_{an} , с учетом переходных вероятностей$1 - P_{0an}$ в цепи Маркова, граф переходов цепи Маркова приведен на рис.16, можем записать:

$$P_{an} = (1 - P_{0an})P_{0У},$$

где P_{an}– вероятность того, что система окажется в n-м поглощающем состоянии.

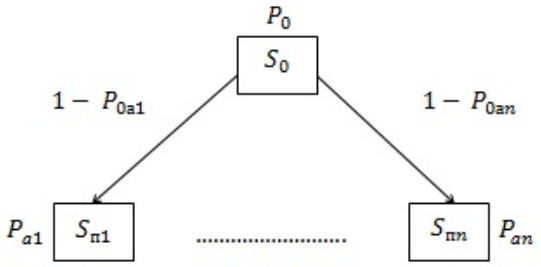


Рис.16. Граф переходов цепи Маркова

С учетом же того, что в каком-то состоянии система всегда должна находиться:

$$P_{0У} + \sum_{n=1}^{N} P_{an} = 1,$$

получаем

$$P_{0У} = 1/(1 + \sum_{n=1}^{N}(1 - P_{0an})).$$

Отметим, что данная формула для моделирования системы с фатальными отказами безопасности корректна в общем случае, поскольку в данных предположениях угрозы атак могут рассматриваться как независимые события (не рассматриваются события (вероятности) одновременного возникновения в системе двух и более угроз атак, создаваемых одними и теми же уязвимостями).

Таким образом, при моделировании системы с отказами и восстановлениями характеристики безопасности необходимо учитывать возможность одновременного появления (в том числе одномоментного) в системе двух и более реальных угроз атак; учет же фатального отказа должен осуществляться в предположении, что в любой момент времени вне зависимости от числа одновременно присутствующих в системе реальных угроз атак только одна из них будет реализована нарушителем.

Теперь построим искомую марковскую модель системы, которая должна учитывать, что реальная угроза атаки с какой-либо вероятностью будет реализована нарушителем, что приведет к невосстанавливаемому – фатальному отказу характеристики безопасности, учитывая

сказанное ранее и учитывая возможность задать в отношении n-й реальной угрозы атаки коэффициент $K_{\text{га}n}$– коэффициент готовности реализовать нарушителем реальную угрозу атаки.

Интересующий нас фрагмент графа состояний случайных процессов системы с невосстанавливаемым– фатальнымотказом характеристики безопасности, построенный для рассмотренного ранее примера системы (граф, для которой при отсутствии фатальных отказов приведен на рис.15), на котором проиллюстрируем важнейшие особенности построенной модели, проиллюстрирован на рис.17.

Замечание. Для того чтобы не загромождать рисунок, на рис.17на графе приведена разметка только интересующих нас для пояснений переходов между состояниями системы.

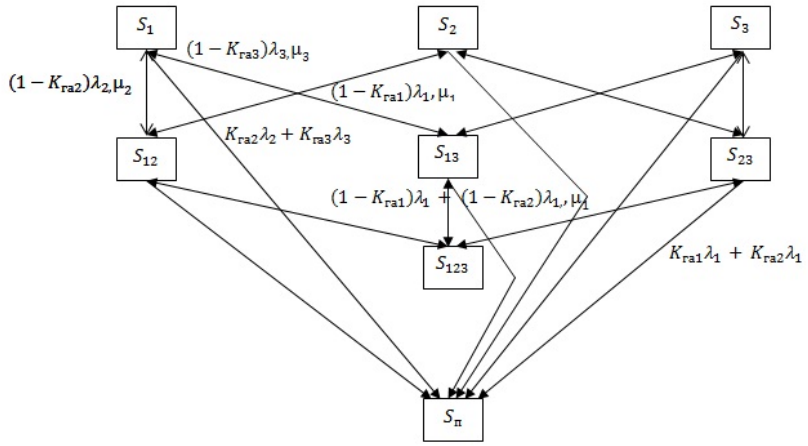


Рис.17. Фрагмент графасистемы состояний случайного процесса для угрозы безопасности информационной системыс фатальным отказом характеристики безопасности

На графе, приведенном на рис.17, включено поглощающеесостояние $S_{\text{п}}$–это состояние, характеризующее невосстанавливаемый – фатальный отказ характеристики безопасности информационной системы (состояние реализации атаки нарушителем на информационную систему) – из него нет переходов.

На графе, представленном на рис.17, следует акцентировать внимание на переходах между следующими состояниями:S_1 и $S_{\text{п}}$,S_{23}и $S_{\text{п}}$, которые обусловливаются наличием в системе угроз атак, зависимых по уязвимостям. Особенность перехода из S_1 в $S_{\text{п}}$ обусловливается тем, что первая уязвимость создает угрозу сразу обеих атак (угрозы этих атак зависимы по первой уязвимости), как следствие, интенсивность перехода из S_1 в $S_{\text{п}}$ определяется как $K_{\text{га}2}\lambda_2 + K_{\text{га}3}\lambda_3$.Особенность же перехода из S_{23} в $S_{\text{п}}$ обусловливается тем, что, как ранее отмечали, при моделировании необходимо учитывать, что в любой момент времени вне зависимости от числа одновременно присутствующих в системе реальных угроз атак только одна из них будет реализована нарушителем. Состояние S_{23} характеризуется тем, что выявлены и не устранены

вторая и третья уязвимости, как следствие, выявление первой уязвимости приводит с соответствующими вероятностями к реализации первой либо второй атаки, поэтому интенсивность перехода из S_{23} в $S_{\text{п}}$опять же определяется как $K_{\text{га1}}\lambda_1 + K_{\text{га2}}\lambda_2$.

4. Укрупненная марковская модель угрозы безопасности информационной системы как системы с фатальным отказом характеристики безопасности.

Применительно к системе с фатальным отказом может быть построена (в данном случае это корректно, поскольку, как отмечали ранее, только одна из реальных угроз атак в любой момент времени реализуется нарушителем) укрупненная марковская модель, граф системы состояний случайного процесса которой представлен на рис.18.Интенсивности перехода в поглощающее состояние в данном случае определяются интенсивностями возникновения реальных угроз атакλ_{an} и коэффициентами готовности реализовать нарушителем реальную угрозу атаки$K_{\text{га}n}$, n = 1,…,N.

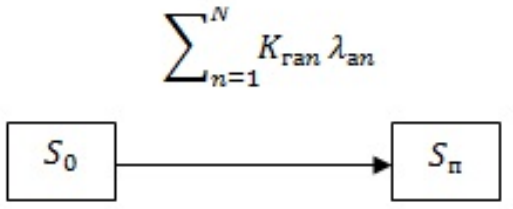


Рис.18. Граф системы состояний случайного процесса для угрозы безопасности информационной системы с фатальным отказом для укрупненной марковской модели

Используя данную модель для угрозы безопасности информационной системы, может быть определена вероятность (коэффициент готовности) того, что система готова к безопасной эксплуатации в отношении угрозы безопасности информационной системы$P_{0\text{у}}(t)$, и среднее время наработки системы до отказа характеристики безопасности (система с фатальным отказом) – до реализации на нее (с эксплуатацией одной из угроз атак, создающих угрозу безопасности информационной системы) успешной атаки нарушителем,$T_{\text{д0у}}$:

$$P_{0\text{у}}(t) = e^{-\sum_{n=1}^{N} K_{\text{га}n}\lambda_{an}t}$$

$$T_{\text{д0у}} = 1/\sum_{n=1}^{N} K_{\text{га}n}\,\lambda_{an}$$

Данная укрупненная модель крайне важна при решении задачи проектирования системы защиты информационной системы, что обусловливается возможностью существенного упрощения решения соответствующих задач моделирования. Упрощение достигается за счет следующего. Угроза безопасности информационной системы на практике для сложных информационных систем создается большим число угроз атак. Это обусловливает возможную

высокую сложность построения марковской моделиугрозы безопасности информационной системы как системы с отказами, восстановлениями и фатальным отказом характеристики безопасности.Использование же укрупненной марковской модели угрозы безопасности информационной системы как системы с фатальным отказом характеристики безопасности позволяет вместо одной очень сложной модели строить много (по числу угроз атак, создающих угрозу безопасности информационной системы) в разы (если не на порядки) более простых моделей –укрупненных марковских моделей угрозы атаки как систем с отказами и восстановлениями характеристики безопасности с целью расчета значений параметра угроз атак λ_{an}, $n = 1,\ldots,N$. Таким образом, практическое использование рассмотренной укрупненной модели направлено на реализацию одного из основополагающих в теории оптимизации методов снижения вычислительной сложности решения задачи за счет сведения решения одной очень сложной задачи к решению множества задач, характеризуемых существенно меньшей сложностью решения.

Замечание. При моделировании системы с восстанавливаемым фатальным отказом (речь идет о нарушении целостности и доступности обрабатываемой информации) в предположении, что восстановление осуществляется с некоторой интенсивностью $\mu_в$ (в первом случае восстанавливается доступность обрабатываемой информации, во втором случае – собственно данные, которые несанкционированно удалены или модифицированы), для определениятребуемых характеристик в укрупненную марковскую модель угрозы безопасности информационной системы как системы с фатальным отказом характеристики безопасности, граф системы состояний которой приведен на рис.18, следует включить переход из состояния $S_п$ ($S_п$ уже становится не поглощающим состоянием) в состояние $S_о$ с интенсивностью $\mu_в$.

Вероятность (коэффициент готовности) того, что система готова к безопасной эксплуатации в отношении угрозы безопасности информационной системы$P_{0у}$ и среднее время наработки системы на фатальный отказ характеристики безопасности (система с восстанавливаемым фатальным отказом) – до реализации на нее (с эксплуатацией одной из угроз атак, создающих угрозу безопасности информационной системы) успешной атаки нарушителем, $T_{0у}$ могут быть определены в данном случае следующим образом:

$$P_{0у} = \mu_в / (\sum_{n=1}^{N} K_{гаn} \lambda_{an} + \mu_в)$$

$$T_{0у} = 1 / \sum_{n=1}^{N} K_{гаn} \lambda_{an}$$

1.7. Моделирование угрозы безопасности информационной системы с использованием аппроксимирующих функций угроз атак

Ранее был изложен подход к моделированию системы угрозы атаки с использованием аппроксимирующей функции:

$$P_{\text{Аya}}(t) = (((1/(1-K_{\text{га}}))^{t/T_{\text{0ya}}} - 1)(1-K_{\text{га}})^{t/T_{\text{0ya}}},$$

использование которой позволяет определить вероятность возникновения реальной угрозы атаки $P_{\text{уа}}$на конкретную информационную систему с учетом готовности реализации этой атаки нарушителем в момент времени *t* (на интервале времени *t*) эксплуатации информационной системы. Таким образом, применительно к каждой *n*-й угрозе атаки можно построить ее аппроксимирующую функцию $P_{\text{Аya}n}(t)$. Ранее показали, что при оценке характеристики безопасности информационной системы в целом вероятностью реализации в системе нарушителем одновременно двух и более атак можно пренебречь. С учетом сказанного и, исходя из того, что с вероятностью $P_{\text{Аya}n}(t)$, n =*1,…,N,* в системе появится *n*-я реальная угроза атаки, коэффициент готовности (вероятность) реализации которой нарушителем $K_{\text{га}}$, для вероятности перехода системы из безопасного состояния, в котором она находится в момент времени *t*с вероятностью $P_{\text{0у}}(t)$, можем записать:

$$P_{\text{0у}}(t) = 1/(1 + \sum_{n=1}^{N} P_{\text{Аya}n}(t))$$

Величина $1-P_{\text{0у}}(t)$ является вероятностью фатального отказа в момент времени *t* (на интервале времени *t*).

Отметим, что данный подход к моделированию также предполагает использование укрупненной марковской модели угрозы атаки как системы с отказами и восстановлениями характеристики безопасности с целью расчета значений характеристики угроз атак$T_{\text{0ya}n}$, n = *1,…,N.*

Таким образом, представленные математические модели позволяют всесторонне исследовать характеристики угроз уязвимостей, угроз атак, угроз безопасности информационной системы, в том числе применительно к решению задачи проектирования системы защиты конкретной информационной системы. Их принципиальным достоинством является возможность моделирования характеристик безопасности без применения каких-либо экспертных оценок.

2. ЗАДАЧИ И МЕТОДЫФОРМАЛЬНОГОПРОЕКТИРОВАНИЯСИСТЕМЗАЩИТЫ ИНФОРМАЦИОННЫХСИСТЕМ

2.1. Общие положения

При формальном проектировании системы защиты информационной системы решаются две взаимосвязанные задачи [23]: определение набора функций (решаемых задач защиты информации) системы защитыиформирование требований к значениям параметровбезопасности системы защиты $\lambda_{\text{сзи}}$ и $\mu_{\text{сзи}}$.Исходными же данными при решении задачи проектирования системы защиты информационной системы являются орграф угрозы безопасности информационной системы, который в обязательном порядке должен быть построен, в противном случае невозможно определить функции проектируемой системы защиты и требования (ограничения) к значениям соответствующих характеристик безопасности защищенной информационной системы.

Исходно подобный орграф имеет вид, проиллюстрированный на рис.19, и представляет собою потенциальные угрозы атак на защищаемую информационную систему, представленные через создающие их последовательности угроз уязвимостей.

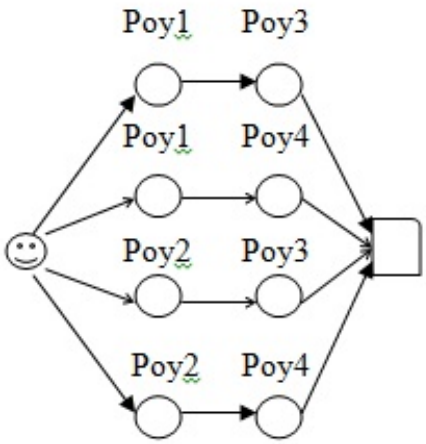


Рис.19. Исходный орграф угрозы безопасности информационной системы

Отметим, что формальное проектирование не дает ответа на вопрос, как эффективно решить ту или иную задачу защиты, как технически реализовать нивелирование той или иной угрозы уязвимости. Эти вопросы рассматриваются в [28].В данном случае решается задача определения того, какие задачи защиты информации должны быть решены в защищенной информационной системе и задача формирования требований к значениям параметров безопасности проектируемой системы защиты.

2.2. Метод формального проектирования системы защиты в части формирования требований к оптимальному набору решаемых задач защитыв информационной системе

Ранее была введена количественная мера актуальности угрозы уязвимости в информационной системе, определяемая тем, каким количеством актуальных угроз атак на информационную систему используется эта угроза уязвимости, соответственно, от какого количества угроз атак защищается информационная система при нивелировании средством защиты данной угрозы уязвимости. Актуальность угрозы уязвимости для информационной системы количественно оценивается с использованием коэффициента актуальности угрозы уязвимости k:

$$k = US,$$

где U – число актуальных угроз атак, входящих в вершину уязвимости на орграфе, S–число актуальных угроз атак, исходящих из вершины уязвимости на орграфе безопасности информационной системы. При этом чем больше для угрозы уязвимости значение коэффициента k, тем актуальнее угроза данной уязвимости для нивелирования ее системой защиты в информационной системе.

Замечание. Данную меру позволила ввести и обосновать введенная интерпретация угрозы безопасности информационной системы при сведении исходного орграфа угрозы безопасности информационной системы к приведенному.

Данный подход к количественному оцениванию актуальности уязвимости положен в основу метода формального проектирования системы защиты информационной системы [23], направленного на определение оптимального набора задач защиты, решаемых проектируемой для какой-либо конкретной информационной системы защиты информации (далее СЗИ).

Далее, говоря о СЗИ, будем понимать, что она состоит из набора средств защиты, каждое из которых решает соответствующую задачу защиты информации: нивелирует соответствующую угрозу уязвимости, т.е. задача проектирования в данном случае сводится к определению оптимального набора средств защиты.

Замечание. При функциональном проектировании СЗИ в части формирования требований к решаемому ею набору задач защиты информации достаточно рассматривать приведенный граф угрозы безопасности информационной системы (не требуется «взвешивания» вершин).

Проектирование с целью выбора оптимального набора средств защиты – набора актуальных угроз уязвимостей, которые должны нивелироваться системой защиты, реализуется выполнением следующей итерационной процедуры. Сначала строится приведенный орграф угрозы безопасности защищаемой информационной системы – информационной системы, для

которой проектируется СЗИ. На каждой последующей итерации анализируется приведенный граф угрозы безопасности информационной системы – граф совокупности угроз атак (исходим из того, что в отношении каждой из этих атак должна быть реализована защита), при этом для каждой угрозы уязвимости рассчитывается значение коэффициента ее актуальности *k*. Из условия *max*kвыбирается наиболее актуальная угроза уязвимости, эта угроза уязвимости должна нивелироваться соответствующим средством защиты.

В случае равенства значения этой метрики для нескольких вершин выбирается та из них, у которой на исходном (перед началом выполнения процедуры проектирования) графе значение коэффициента *k* было больше. Это обусловливается следующими очевидными соображениями. При выборе подобной вершины (при нейтрализации соответствующей угрозы уязвимости средством защиты) снижаются требования к характеристикам выбранных ранее средств защиты, применение которых позволило исключить соответствующие входы/выходы для выбираемой вершины на данной итерации, поскольку данное средство защиты будет выступать в качестве резервирующего элемента для соответствующих средств защиты, выбранных на предыдущих этапах. В случае равенства и этого значения искомая вершина выбирается произвольным образом.

Для перехода к следующей итерации из исходного для данной итерации графа исключаются все угрозы атак (исключаются соответствующие вершины и дуги), для осуществления которых должна использоваться выбранная на данной итерации угроза уязвимости. Процедура продолжается до тех пор, пока из исходного графа не будут исключены все угрозы атак. Результатом выполнения описанной итерационной процедуры проектирования будет выявление актуальных угроз уязвимостей – угроз уязвимостей, которые должны в системе нивелироваться, т.е. определение набора задач защиты (набора средств защиты), которые должны решаться проектируемой СЗИ для информационной системы.

Проиллюстрируем применение данного метода проектирования на примере исходного приведенного графа, представленного на рис.20.а.

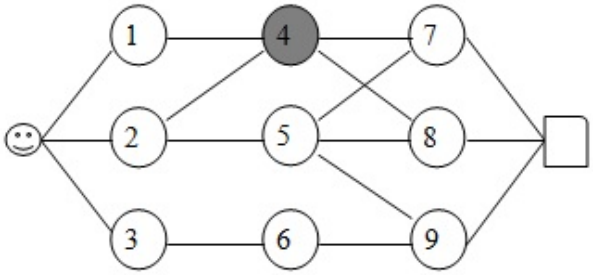
На первой итерации по максимальному значению коэффициента *k* выбирается 4-я вершина – выбрано первое средство защиты, которое должно нивелировать 4-ю угрозу уязвимости.

В результате преобразования исходного графа (исключения 4-й вершины) получаем преобразованный граф – исходный граф для второй итерации, приведенный на рис.20.б. Используя тот же критерий оптимальности, выбираем на этой итерации пятую вершину – выбрано второе средство защиты, которое должно нивелировать 5-ю угрозу уязвимости.

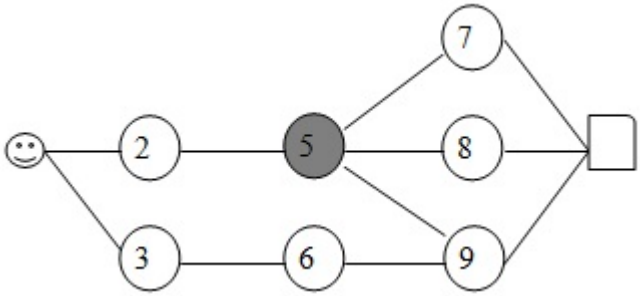
В результате преобразования исходного для этой итерации графа (исключения 5-й вершины) получаем исходный граф для третьей итерации, приведенный на рис.20.в. На этом

графе три вершины 3,6,9 характеризуются одинаковым значением коэффициента*k*; однако 9-я вершина (при прочих равных условиях) на исходном графе имела максимальное из сравниваемых вершин значение коэффициента *k*, поэтому на этой итерации выбираем 9-ю вершину – выбрано третье средство защиты, которое должно нивелировать угрозу 9-й уязвимости.

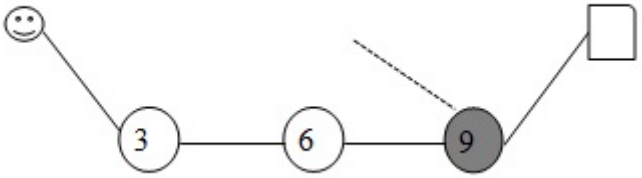
Процедура проектирования завершена. В результате ее выполнения для информационной системы, характеризуемой исходно заданным графом угрозы безопасности, определен состав системы защиты: она должна содержать в своем составе средства защиты, нивелирующие угрозы 4,5 и 9 уязвимостей, т.е. определены функциональные задачи системы защиты – нивелирование угроз 4,5 и 9 уязвимостей.



а. Исходный приведенный граф. Первая итерация



б. Вторая итерация



в. Третья итерация

Рис.20. Иллюстрация применения метода функционального проектирования

Размещаем на исходном графе актуальных атак, см. рис.20, вершины полученных при проектировании средств защиты (31, 32, 33), предназначенные для нивелирования выбранных

угроз уязвимостей (четвертой, пятой и девятой), в результате чего получаем приведенный граф угрозы безопасности защищенной информационной системы, представленный на рис.21.

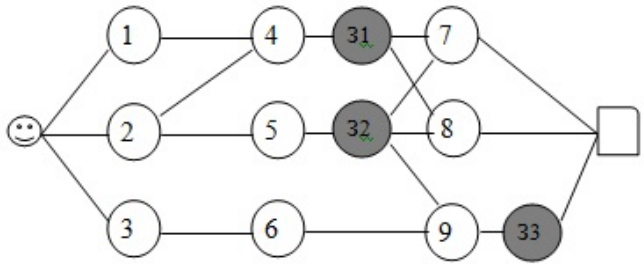


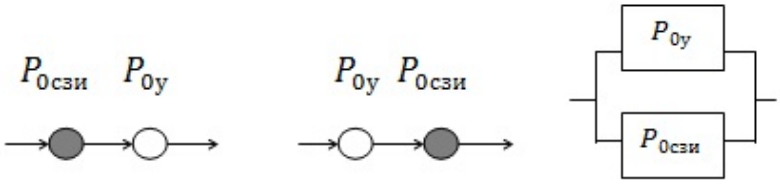
Рис.21. Граф угрозы безопасности защищенной информационной системы

Таким образом, данный метод проектирования позволяет сформировать требования к оптимальному набору задач защиты, решаемых проектируемой СЗИ для защищенной информационной системы.

Теперь несколько слов по поводу включения в граф вершин средств защиты информации. Возможны два способа, будем их отображать так, как это сделано на рис.22а. С точки зрения практической реализации системы защиты эти способы кардинально различаются. Первый способ предполагает непосредственно нивелирование средством защиты угрозы уязвимости, например, предотвращение возможности установки интерактивным пользователем на компьютер исполняемого файла [11].Альтернативный же способ не предполагает как такового нивелирования угрозы уязвимости – реализуется защита, направленная на предотвращение последствий (на снижение возможных последствий) от атак на угрозу уязвимости, например, предотвращается возможность исполнения созданных в процессе работы интерактивными пользователями файлов [24]. Другой пример альтернативных решений – это предотвращение возможности наделения критичных (предоставляющие подобные возможности, например, с использованием макросов или апплетов) приложений вредоносными свойствами и предотвращение последствий от атак на защищаемые ресурсы в предположении, что критичное приложение наделено соответствующими вредоносными возможностями [26]. То же можно сказать и в отношении получения нарушителем системных прав(предотвратить подобную возможность [25] либо предотвратить последствия от совершения подобной атаки), реализовав разграничительную политику доступа к обрабатываемой информации (данным) для системного пользователя [27].

Применение альтернативных способов защиты от атак на уязвимость, проиллюстрированных на рис.22.а, с точки зрения обеспечиваемого уровня безопасности в отношении атаки на уязвимость, естественно, при корректном решении соответствующей задачи защиты эквивалентны. Для подтверждения сказанного вновь обратимся к рассмотренной

ранее интерпретации угрозы атаки, но уже при условии реализации системы защиты в информационной системе.



а. Схемы включения вершины средства защитыб. Схема резервирования

Рис.22. Схемы включения в орграф угрозы атаки вершин средств защиты и схема резервирования

Как видим, с точки зрения проектирования системы защиты альтернативные схемы, представленные на рис.22.а, эквивалентны, т.к. образуют одну и ту же схемупараллельного резервирования, см. рис.22.б, т.е. в общем случае эквивалентны и альтернативные способы реализации защиты, отличие может состоять лишь в значениях параметров безопасности $\lambda_{сзи}$и $\mu_{сзи}$, характеризующих эффективность средств защиты, в том числе характеризующих возможность их обхода нарушителем.

2.3. Метод динамического программирования, используемый для минимизации угроз атак, исследуемых при формировании требований к значениям характеристик и параметров безопасности средств защиты

Ранее были приведены математические модели, которые могут использоваться при проектировании СЗИ (в частности входящих в ее состав средств защиты информации), в том числе для формирования требований к значениям ее характеристик и параметров безопасности. Основная проблема проектирования в части решения рассматриваемой задачи состоит в том, что на практике граф угрозы безопасности информационной системы будет содержать достаточно много угроз атак, что обусловливает высокую сложность задачи моделирования.

Метод динамического программирования [6] в рассматриваемом случае позволяет минимизировать набор исследуемых при проектировании СЗИ угроз атак, упростив тем самым задачу проектирования, обеспечивая при этом корректность формируемыхпри проектировании требований к характеристикам и параметрам безопасности средств защиты. Данная задача проектирования уже решается на модифицированном орграфе атак – на орграфе, в состав которого включены вершины системы защиты, которые необходимо соответствующим образом "взвесить".

Метод динамического программирования состоит в решении задачи проектирования в два этапа[23]. На первом этапе оптимизируется исходный приведенный модифицированный орграф (с включенными в орграф вершинами средств защиты). Оптимизация состоит в

последовательном исключении из графа путей (вершин и ветвей, за исключением вершин средств защиты), образующих "неактуальные угрозы атак для формирования требований к средствам защиты". Для этого на орграфе последовательно осуществляется анализ путей орграфа из конца в начало: на каждом шаге находятся вершины, имеющие более одного выхода, из которых выходит более одной дуги. Для каждого из образующих найденной вершиной путей (пусть*V, v = 1,..., V*) вычисляется значение критерия выбора "актуальной угрозы атак для формирования требований к средствам защиты", представляющего собою вероятность того, что защищенная информационная система готова к безопасной эксплуатации в отношении угрозы атаки $P_{0азисv}$, образующей*v*-й путь из выбранной вершины, последовательно использующей R_vугроз уязвимостей, r_v =1,…,R_v, определяемая следующим образом:

$$P_{0азисv} = 1 - \prod_{r_v=1}^{R_v}(1 - P_{0yr_v}),$$

где P_{0yr_v}– вероятность отсутствия в системе r_v-й уязвимости (информационная система готова к безопасной эксплуатации в отношении r_v-й уязвимости).

"Актуальная угроза атак для формирования требований к средствам защиты" применительно к рассматриваемой вершине выбирается из следующего условия:

$$P_{0азисvmin} = \min \{P_{0азисv}, v = 1,..., V\}$$

"Неактуальные угрозы атак для формирования требований к средствам защиты" на каждом шаге исключаются из дальнейшего рассмотрения, что реализуется удалением на орграфе образующих угрозы этих атак вершин и путей.

На втором этапе уже для "актуальных угроз атак для формирования требований к средствам защиты" решаются соответствующие задачи моделирования с целью формирования требований к характеристикам и параметрам средств защиты.

Проиллюстрируем применение рассмотренного метода проектирования для приведенного модифицированного (с включенными в него вершинами средств защиты) графа угрозы безопасности защищенной информационной системы, приведенного на рис.21 (это полученный нами граф в результате формального проектирования СЗИ, см. рис.20.а), при этом «взвесим» вершины графа в соответствии с табл.6.

Таблица 6

Заданные значения P_{0yr}для вершин орграфа

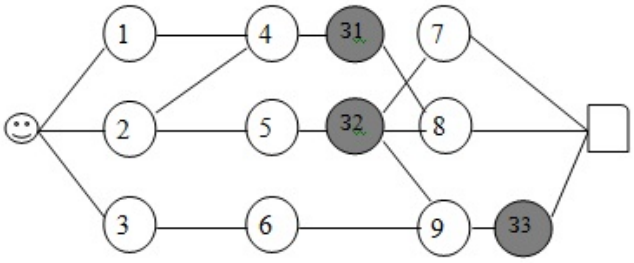
Заданные значения	**Вершины графа**											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**31**	**32**	**33**
P_{0yr}	0,2	0,3	0,5	0,6	0,3	0,7	0,4	0,2	0,1	Требуется определить		

Итерационная процедура оптимизации проиллюстрирована на рис.23.Будем рассматривать граф из конца в начало в поисках вершин, имеющих более одного выхода, будем анализировать граф сверху вниз. Первая вершина, которую мы найдем, будет вершина 31. Из вершины 31 можем пройти по графу в вершины 7 и 8 – эти пути можем рассматривать в качестве альтернативных. Обратимся к табл.1, видим, что более критична из этих вершин вершина 8, т.к. ее значение P_{0yr} меньше. Как следствие, требование к значению P_{0yr} для вершины 31 на рассматриваемой части графа будет формироваться вершиной 8 (выполнив требование применительно к вершине 8, соответственно выполним и требование применительно к вершине 7).Это позволяет нам исключить соответствующие пути на графе, образующие "неактуальную угрозу атак для формирования требований к средствам защиты" (через вершину 7), для дальнейшего анализа, см. рис.23.а.

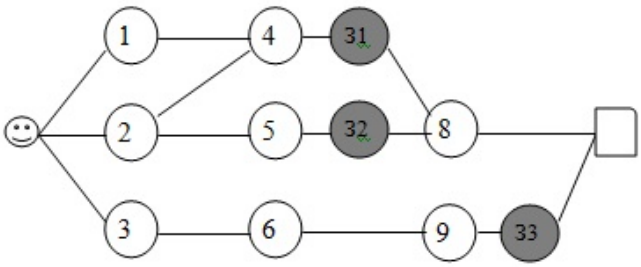
Следующей выбранной нами вершиной будет вершина 32, из которой можно пройти через вершины 7либо 8, либо через последовательность вершин: 9, 33. Обратимся к табл.1 и определим, какая вершина формирует требования к вершине 32. Как видим, это вершина 8.

Замечание. По понятным причинам из графа не должны исключаться вершины средств защиты информации.

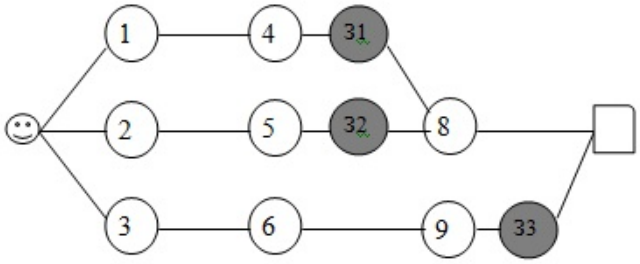
С учетом этого выполним дальнейшее преобразование графа, см. рис.23.б. Следующей искомой вершиной будет вершина 2, требования для которой формируются, в соответствии с табл.6, вершиной 5. Соответствующим образом преобразованный граф приведен на рис.23.в. Как видим, третий шаг оптимизации последний, поскольку на каждом пути присутствует вершина средства защиты информации, которую мы не можем исключать из графа.



а. Первый шаг оптимизации



б. Второй шаг оптимизации



в. Третий шаг оптимизации

Рис.23. Иллюстрация итерационной процедуры проектирования

Таким образом, угрозами атак, формирующими требования к средствам защиты, будут угрозы атак, определяемые следующими последовательностями эксплуатируемых угроз уязвимостей, см. рис.23.в: 1,4, 31,8; 2,5, 32,8; 3,6,9, 33.

Замечание. В том случае, если все средства защиты включаются в состав одной СЗИ (требуется определить характеристики и параметры СЗИ) из дальнейшего рассмотрения при оптимизации модифицированного графа могут исключаться и угрозы атак, содержащие в своем составе вершины средств защиты информации. Например, сравним две последовательности эксплуатируемых угроз уязвимостей, см. рис.23.в: 1,4, 31,8 и 2,5,32,8. Видим, что последовательность 1,4, 31,8 может быть исключена из дальнейшего рассмотрения при условии, что для средства защиты, определяемого вершиной 31, требование к характеристике безопасности будет формулироваться следующим образом: $P_{0y31} \geq P_{0y32}$.

2.4. Формирование требований к значениям характеристик и параметров безопасности средств защиты

Реализация первого этапа метода динамического программирования позволяет определить "актуальные угрозы атак для формирования требований к средствам защиты", т.е. те угрозы атак, в отношении которых при проектировании СЗИ необходимо решить соответствующие задачи моделирования, используя представленные ранее математические модели. Будем рассматривать построение и использование моделей в предположении, что в отношении угроз атак ведется соответствующая статистика, по аналогии с тем, как она сейчас ведется в отношении угроз уязвимостей, т.е. в отношении угроз атак ранее определены (смоделированы)значения их основных характеристик безопасности угрозы атакиλ_a иμ_a.

Замечание. Если для каких-либо "актуальных угроз атак для формирования требований к средствам защиты" не определены значения основных параметров и характеристик безопасности, то для каждой из них следует построить марковскую и укрупненную марковскую модели угрозы атаки как системы с отказами и восстановлениями характеристики безопасности с целью определения значений основных параметров безопасности угрозы

атаки λ_a и μ_a. Отметим, что в данной модели вершины средств защиты не учитываются, например, моделируются угрозы атак, определяемые следующими последовательностями эксплуатируемых угроз уязвимостей, см. рис.23.в: 1,4,8; 2,5,8; 3,6,9.

На следующем этапе проектированиястроится математическая модель угрозы атаки уже защищенной информационной системы, граф системы состояний случайного процесса (марковского процесса) для которой представлен на рис.24. В предположении, что угрозы атаки на информационную систему и на СЗИ независимы (а это одно из основополагающих требований к реализации эффективной защиты), данная модель защищенной информационной системы корректна.

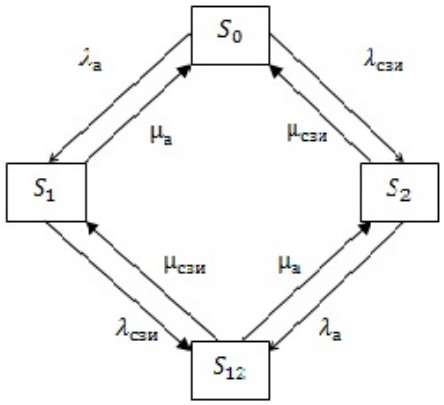


Рис.24. Граф системы состояний случайного процесса для угрозы атакизащищенной информационной системы, как системы с отказами и восстановлениями характеристики безопасности

Задавая значения параметров средства защиты $\lambda_{сзи}$ и $\mu_{сзи}$, можно рассчитать значения требуемых характеристик и параметров безопасности угрозы атаки защищенной информационной системы как системы с отказами и восстановлениями характеристики безопасности в отношении угрозы атаки.

Система линейных алгебраических уравнений, описывающих стационарный режим для данной модели:

$$\begin{cases} (\lambda_a + \lambda_{сзи})P_0 = \mu_a P_1 + \mu_{сзи} P_2 \\ (\lambda_{сзи} + \mu_a)P_1 = \lambda_a P_0 + \mu_{сзи} P_{12} \\ (\lambda_a + \mu_{сзи})P_2 = \lambda_{сзи} P_0 + \mu_a P_{12} \\ (\mu_a + \mu_{сзи})P_{12} = \lambda_{сзи} P_1 + \lambda_a P_2 \end{cases}$$

Коэффициент готовности защищенной информационной системы $К_{гзис}$, соответственно, вероятность готовности к безопасной эксплуатации защищенной информационной системы в отношении угрозы атаки $P_{0азис}$рассчитывается следующим образом:

$$К_{гзис} = P_{0азис} = \frac{\mu_a \mu_{сзи} + \lambda_a \mu_{сзи} + \lambda_{сзи} \mu_a}{(\lambda_a + \mu_a)(\lambda_{сзи} + \mu_{сзи})}$$

Интенсивность $\lambda_{азис}$ параметра потока отказов,ω (для стационарного участка) – поток возникновения реальной угрозы в защищенной информационной системе определяется следующим образом:

$$\lambda_{азис} = \omega = P_1\lambda_{\text{сзи}} + P_2\lambda_a,$$

где P_1, P_2– вероятности соответствующих состояний S_1, S_2 , см. рис.24.

Среднее время наработки на отказ (восстанавливаемая система) характеристики безопасности в защищенной информационной системе в отношении соответствующей угрозы атаки $T_{0\text{уазис}}$:

$$T_{0\text{уазис}} = 1/\lambda_{\text{азис}}$$

Оценить сложность реализации исследуемой угрозы атаки на защищенную информационную систему$S_{азис}$ можно следующим образом:

$$S_{азис} = S_a + S_{асзи},$$

где S_a – сложность реализации угрозы соответствующей атаки на незащищенную информационную систему, $S_{\text{асзи}}$– сложность реализации угрозы атаки на СЗИ ($S_{а\text{сзи}} = I(P_{0а\text{сзи}})$).

Таким образом, можно рассчитать значения характеристик угроз безопасности защищенной информационной системы в отношении каждой "актуальной угрозы атаки для формирования требований к средствам защиты".

Последующее проектирование осуществляется с использованием исходно заданных требований (ограничений) к значениям соответствующих характеристик безопасности защищенной информационной системы.

В простейшем случае проектирование СЗИ может осуществляться с заданием требования к минимальной сложности реализации атаки в защищенной информационной системе $min\ S_{азис}$. Проиллюстрируем решение подобной задачи проектирования на представленном выше примере применительно к исследуемому ранее орграфу безопасности информационной системы.

Получим для угроз атак, определяемых следующими последовательностями эксплуатируемых угроз уязвимостей, см. рис.23.в: 1,4, 31,8; 2,5, 32,8; 3,6,9, 33,искомые расчетные формулы:

$$P_{0азис1} = 1 - (1 - P_{0у1})(1 - P_{0у4})(1 - P_{0у31})(1 - P_{0у8})$$

$$P_{0азис2} = 1 - (1 - P_{0у2})(1 - P_{0у5})(1 - P_{0у32})(1 - P_{0у8})$$

$$P_{0азис3} = 1 - (1 - P_{0у3})(1 - P_{0у6})(1 - P_{0у33})(1 - P_{0у9})$$

Пусть исходно задано требование к характеристикам сложности реализации угроз атак в информационной системе: не менее некоторого значения$\min S_{\text{азис}}$, исходя из которого может

быть определено значение вероятности готовности (коэффициент готовности) информационной системы к безопасности эксплуатации в отношении любой угрозы атаки $P_{0a_{min}}$.

Задав $P_{0азис1}$, $P_{0азис2}$,$P_{0азис3}$ равными требуемому значению $P_{0a_{min}}$, можно рассчитать значения искомых величин P_{0y31}, P_{0y32}, P_{0y33}.

Например, для обеспечения в информационной системе, описываемой орграфом, приведенным на рис.21(соответствующие характеристикиугроз уязвимостей заданы в табл.6), требования к значению вероятности готовности защищенной информационной системы к безопасной эксплуатации в отношении любой из угроз атак не ниже значения$P_{0a_{min}}$ = 0,99 ($S_{amin} = 6{,}64$). Необходимо использование средств защиты со следующими характеристиками безопасности: P_{0y31} =0,961, P_{0y32} =0,974, P_{0y33} =0,923. Естественно, что, если данные средства защиты входят в состав одной СЗИ, то требование к характеристике безопасности СЗИ определяется следующим образом: $P_{0усзи}$ =0,974 ($S_{асзи}$ =5,27). Определенные значения соответствующей характеристики безопасности$P_{0усзи}$ уже позволяют сформировать требования к значениям соответствующих параметров безопасности: к интенсивности возникновения (выявления) и устранения угроз уязвимостей системы (средств) защиты– $\lambda_{\text{сзи}}$ и$\mu_{\text{сзи}}$, исходя из того, что (естественно, что для СЗИ следует рассматривать условие $\rho_{\text{сзи}} \leq 0{,}2$):

$$P_{0усзи} = 1 - \rho_{\text{сзи}},$$

где

$$\rho_{\text{сзи}} = \lambda_{\text{сзи}}/\mu_{\text{сзи}}.$$

В общем случае при проектировании СЗИ могут задаваться следующие ограничения на значения характеристик безопасности защищенной информационной системы в отношении угроз атак:минимальное значение вероятности готовности к безопасной эксплуатации системы в отношении угрозы атаки$min\, P_{0азис}$ (или стационарный коэффициент готовности$min\, K_{гзис}$) и минимальное среднее время наработки системы до отказа характеристики безопасности (система с фатальным отказом) – до реализации на нее успешной атаки (реализации угрозы атаки нарушителем),$minT_{\text{д0уазис}}$.

Для использованияпри проектированииограничений на данные характеристики безопасности в отношении угрозы атакиуже требуется построить математическую модель угрозы атаки защищенной информационной системы как системы с отказами, восстановлениями и фатальным отказом характеристики безопасности, граф системы состояний случайного процесса (марковского процесса) для которой представлен на рис.25. Если же речь идет о таких характеристиках безопасности, как нарушение доступности и целостности информации (восстанавливаемый фатальный отказ), тов граф, представленный на рис.25, необходимо включить переход из состояния $S_{3.2}$ ($S_{3.2}$ уже становится непоглощающим

состоянием) в состояние S_o с интенсивностью $\mu_в$ (интенсивность восстановления информационной системы после реализации на нее успешной атаки, в частности, системных и/или прикладных программных средств и/или несанкционированно удаленных или модифицированных данных).

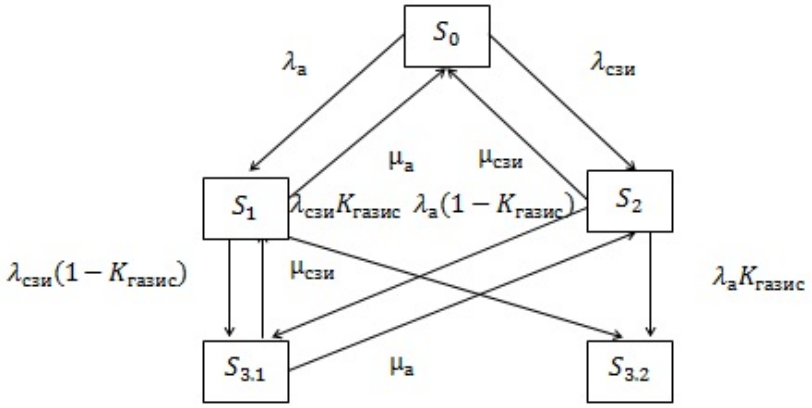


Рис.25. Граф системы состояний случайного процесса для угрозы атакизащищенной информационной системы как системы с фатальным отказом характеристики безопасности

В данном случае при проектировании в обязательном порядке исходно должно задаваться значение характеристики $S_{ан}$ – характеристика максимальной сложности реализованных (в том числе и отраженных) в подобной информационной системе атак, что необходимо для расчета коэффициента готовности нарушителя осуществить атаку сложности $S_а$ на информационную систему, для которой проектируется система защиты,$K_{газис}$.Для СЗИ сложность реализации атаки $S_{асзи}$, с учетом чегозначение коэффициента $K_{гасзи}$ определяется следующим образом:

$$K_{газис} = \begin{cases} \dfrac{S_{ан}}{S_а + S_{асзи}}, \text{если } S_{ан} < S_а + S_{асзи} \\ 1, \quad \text{если } S_{ан} \geq S_а + S_{асзи} \end{cases}$$

Используя данные модели, можно сформировать требования к значениям соответствующих параметров безопасности: к интенсивности возникновения (выявления) и устранения угроз уязвимостей системы (средств) защиты – $\lambda_{сзи}$ и $\mu_{сзи}$ ($\lambda_а$ и $\mu_а$ заданы либо соответствующим образом рассчитываются), при которых выполняются заданные при проектировании СЗИ ограничения на характеристики безопасности в отношении угроз атак: $minP_{0азис}$($minK_{гзис}$) и $minT_{д0уазис}$.

Для экономического обоснования применения проектируемой СЗИ должна быть построена соответствующая модель с использованием аппроксимирующей функции. В этом случае в отношении исследуемой угрозы атаки можно определить вероятность возникновения

реальной угрозы атаки $P_{уазис}$на защищенную информационную систему с учетом готовности реализации этой атаки нарушителем в любой момент времени t эксплуатации информационной системы – вероятность фатального отказа$P_{\text{Ауазис}}(t)$, как следствие, и величину потенциальных потерь $R_{C_{\text{Уинфзис}}}(t)$:

$$R_{C_{\text{Уинфзис}}}(t) = C_{инф} P_{\text{Ауазис}}(t)$$

Аппроксимирующая функция для угрозы исследуемой угрозы атаки на защищенную информационную систему $P_{\text{Ауазис}}(t)$определяется следующим образом:

$$P_{\text{Ауазис}}(t) = (((1/(1 - K_{\text{газис}}))^{t/T_{\text{0уазис}}} - 1)(1 - K_{\text{газис}})^{t/T_{\text{0уазис}}}$$

Выше мы рассмотрели подход к проектированию системы защиты в предположении, что исходно задаются ограничения в отношении угрозы атаки, исходя из того, что в отношении любой из угроз атак на защищенную информационную систему должны выполняться исходно заданные ограничения на значения соответствующих характеристик безопасности. Это позволило минимизировать исходное множество исследуемых потенциальных угроз атак на информационную систему, оперируя только с "актуальными угрозами атак для формирования требований к средствам защиты".

Исходя из того, что угрозу безопасности информационной системы в целом создают N угроз атак с номерами $n=1,...,N$(что определяется исходным для проектирования СЗИ орграфом угрозы безопасности информационной системы), характеристики угрозы безопасности защищенной с использованием спроектированной СЗИ информационной системы, например, граничное (хуже не будет) среднее время наработки до отказа $T_{\text{гр0Узис}}$ – до реализации на нее (с эксплуатацией одной из N угроз атак, создающих угрозу безопасности информационной системы) успешной атаки нарушителем, может быть определена следующим образом:

$$T_{гр0Узис} = 1/NL_{nmax},$$

где

$$L_{nmax} = \max\{ K_{газисd}\lambda_{\text{азисd}}, d = 1, \ldots, D\},$$

а $K_{газисd}$и$\lambda_{\text{азисd}}$ – соответствующие характеристики угроз атак на защищенную (с использованием соответствующих средств защиты) информационную систему, определяемые на множестве "актуальных угроз атак для формирования требований к средствам защиты", с номерами $d=1,...,D$.

Исходные ограничения при проектировании СЗИ могут задаться не в отношении угроз атак, а в отношении угрозы безопасности информационной системы в целом, например, следующим образом:$minT_{гр0Узис}$. В этом случае задача проектирования СЗИ также может быть сведена к задаче проектирования с исходно заданными требованиями к характеристикам безопасности в отношении угроз атак. Осуществляется это следующим образом. Пусть исходно

задано ограничение $minT_{гр0Узис}$ при возможности реализации в системе N угроз атак. Тогда очевидно, что требование к характеристике безопасности в отношении любой из N угроз атак формируются следующим образом:

$$L_{nmax} = 1/NminT_{гр0Узис}$$

Соответствующим образом с учетом этого могут быть сформированы и требования в отношении любой из "актуальных угроз атак для формирования требований к средствам защиты" с номерами $d=1,...,D$ (при выполнении данных требований по отношению к этим угрозам атак, следуя изложенному методу динамического программирования, будут выполнены эти требования и в отношении всех остальных угроз атак, создающих угрозу безопасности защищенной информационной системы):

$$maxK_{газисd}\lambda_{азисd} = 1/NminT_{гр0Узис},$$

где $d = 1, \ldots, D$.

2.5. Эксплуатационное проектирование системы защиты информационной системы

Используя приведенные выше методы и модели можно спроектировать систему защиты и ввести ее в эксплуатацию. Однако имеет место несколько причин, по которым процесс проектирования системы защиты должен в общем случае неоднократно осуществляться (уточняться результаты проектирования СЗИ) при эксплуатации защищенной информационной системы. Будем называть этот процесс эксплуатационным проектированием.

Первая причина вызвана потенциальной возможностью некорректного задания параметров λ,μ, как следствие, некорректного расчета характеристики$P_{0у}$угроз уязвимостей. В первую очередь это возможно при отсутствии существенной статистики по угрозе уязвимости. Изменение значений параметров λ,μугрозы уязвимости по сравнению с исходно сделанными прогнозами при проектировании системы защиты приводит к изменению исходного построенного при проектировании орграфа угрозы безопасности информационной системы в части "взвешивания" соответствующих вершин. Изменение характеристики $P_{0у}$ уязвимости приводит к изменению характеристики P_{0a}угрозы атаки (соответственно$P_{0азис}$ при реализации в информационной системе защиты от этой атаки), как следствие, к изменению значения характеристики $S_а$ на величину ΔS_a. Если обозначить исходную (рассчитанную при проектировании) сложность реализации атаки на информационную систему как $S_{aисх}$, а сложность реализации атаки, рассчитанную в процессе эксплуатации информационной системы, как $S_{aэкспл}$, то для ΔS_a имеем:

$$\Delta S_a = S_{aэкспл} - S_{aисх}$$

Отметим, что характеристика ΔS_a может рассматриваться в качестве так называемой в теории информации прагматической меры количества информации, определяемой в данном случае по формуле:

$$\Delta S_a = log_2(1 - P_{0a\text{исх}}) - log_2(1 - P_{0a\text{экспл}}) = log_2 \frac{(1-P_{0a\text{исх}})}{(1-P_{0a\text{экспл}})},$$

где $P_{0a\text{исх}}$ и $P_{0a\text{экспл}}$– вероятности готовности системы к безопасной эксплуатации в исходный момент времени и в рассматриваемый момент времени эксплуатации системы.

Прагматика данной оценки в рассматриваемом случае состоит в выявлении условий, при которых необходимо изменение требований к средству защиты.

Вторая причина обусловливается появлением новых типов уязвимостей, соответственно, потенциально возможных атак на информационную систему в процессе ее эксплуатации. Это также приводит к необходимости актуализации исходного (взятого за основу при проектировании системы защиты) орграфа угрозы безопасности информационной системы.

Отметим, что новые типы угроз уязвимостеймогут образовываться, в том числе при смене (дополнении) программного обеспечения и соответствующего оборудования, эксплуатируемых информационной системой, а так же при смене отдельных систем защиты.

Данные причины объясняют необходимость систематической оценки (в том числе при смене оборудования или программного обеспечения) актуальности исходного орграфа безопасности информационной системы с проведением, при необходимости, соответствующей его модификации в случаях изменения параметров угроз уязвимостей либо при выявлении новых типов угроз уязвимостей информационной системы (выявлении новых потенциально возможных атак) с соответствующей доработкой системы защиты при выявлении соответствующих условий.

Третья причина уже связана с возможностью изменения характеристики $S_{a\text{н}}$ (количественной характеристики нарушителя) в процессе эксплуатации защищенной информационной системы. Это может быть вызвано как не вполне корректным заданием значения этой характеристики при исходном проектировании системы защиты информационной системы (в том числе за счет некорректного выбора подобной информационной системы– аналога – либо при невозможности ее выбора), так и ростом в процессе эксплуатации системы (по каким-либо причинам) заинтересованности, как следствие, и потенциальных возможностей нарушителя в осуществлении несанкционированного доступа к информации, обрабатываемой в эксплуатируемой защищенной информационной системе.

Это обусловливает целесообразность систематической корректировки модели нарушителя в части актуализации орграфа реализованных (в том числе отраженных) злоумышленником угроз атак на эксплуатируемую защищенную информационную систему. При выявлении существенного изменения значения коэффициента $К_{га}$ (уровень сложности

осуществляемых злоумышленником атак на информационную систему существенно вырос в процессе ее эксплуатации), что критично, поскольку в результате этого могут существенно измениться требования к системе защиты, определяемые характеристикой $P_{0сзи}$,необходимо оценить целесообразность доработки спроектированной системы защиты в части корректности в этих условиях определенных при проектировании требовании к значениям параметров ее безопасности.

Таким образом, эксплуатационное проектирование системы защиты информационной системы требует как непрерывного анализа параметров угроз уязвимостей (с учетом соответствующей обновляемой их статистики) с целью корректировки исходно заданных для них значений и, при необходимости, актуализации значений их характеристик и непрерывного анализа потенциально возможных угроз атак с использованием существующих и вновь выявляемых угроз уязвимостей (что в общем случае не связано с конкретной информационной системой), так и непрерывного анализа сложности угроз атак, реализуемых нарушителем на эксплуатируемую защищенную информационную систему, что уже осуществляется с использованием средств аудита попыток несанкционированного доступа, реализованных в спроектированной и эксплуатируемой системе защиты.

Отметим, что необходимость эксплуатационного проектирования также является принципиальным отличием задач проектирования, решаемых в теории информационной безопасности, от соответствующих задач проектирования, решаемых в теории надежности.

3. ЗАДАЧИ И МЕТОДЫ РЕЗЕРВИРОВАНИЯ ЭЛЕМЕНТОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

3.1. Общие положения

Резервирование является одним из эффективных способов повышения надежности функционирования информационной системы[14], при этом на практике резервируются наиболее критичные к отказу элементы информационной системы, как правило, серверы, на которых концентрируется обработка и хранение обрабатываемых данных[5].

Однако в современных условиях информационные системы, требующие резервирования элементов, т.е. критичные к нарушению характеристики надежности функционирования, подвержены угрозам атак несанкционированного доступа, т.е. критичны и к нарушению характеристики безопасности. Рассмотрим возможности применения резервирования элементов информационной системы применительно к решению задачи повышения уровня ее безопасности. С учетом же того, что для современных информационных систем данные характеристики (характеристика надежности и характеристика безопасности) сопоставимо важны, исследуем возможность комплексного решения задачи резервирования с использованием одних и тех же средств с целью повышения уровня интегрированнойинформационно-эксплуатационнойбезопасностиинформационных систем (и для повышения уровня надежности, и для повышения уровня безопасности в комплексе).

При этом, прежде всего, рассмотрим основные отличия в постановке данных задач резервирования. При резервировании, реализуемом с целью повышения надежности функционирования информационной системы, подразумевается, что исследуемыми событиями выступают отказы, влияющие лишь на одну характеристику – характеристику надежности функционирования системы. При этом отказы зарезервированных элементов в общем случае (не рассматриваем различные техногенные события) можно интерпретировать как независимые события. В информационной безопасности это не так:

1. Исследуемым элементом безопасности является угроза атаки, при этом атаки, в отличие от отказов, никак не могут рассматриваться как независимые события, поскольку атака представляет собою не некое случайное, а осознанное деструктивное воздействие нарушителя безопасности на информационную систему, реализуемое с целью несанкционированного доступа к обрабатываемой в системе информации. Естественно предположить, что, если нарушитель совершил успешную атаку на элемент информационной системы, на резервирующий элемент он в первую очередь попытается совершить аналогичную апробированную им атаку. Как следствие, события деструктивного воздействия на зарезервированные элементы следует рассматривать как зависимые.

2. Информационная безопасность имеет несколько ключевых характеристик, сопоставимо важных при решении задач повышения уровня информационной безопасности систем. К характеристикам информационной безопасности относятся: защита от нарушения конфиденциальности информации (защита от ее хищения), защита от нарушения целостности информации (защита от ее несанкционированной модификации), защита от нарушения доступности информации. В общем случае при реализации защиты информационной системы данные задачи защиты, направленные на обеспечение требуемого уровня этих характеристик, должны решаться в комплексе.

Замечание. Ранее мы исследовали проблемы резервирования собственно средств защиты информации, в результате чего сделали вывод о том, что эффективная защита с использованием резервирования достигается в том случае, если резервируемая и резервирующая системы защиты не зависимы по угрозам уязвимостей. В данном разделе речь идет о резервировании элементов информационной системы, концентрирующих на себе обработку защищаемой информации в первую очередь серверов.

3.2. Задача резервирования элементов системы, решаемая с целью повышения надежности функционирования информационной системы

Рассмотрим задачу, решаемую с целью повышения уровня надежности (отказоустойчивости) функционирования информационной системыпосредством резервирования наиболее критичных к отказам элементов.

Резервирующие элементы при этом в простейшем случае включаются по схеме параллельного резерва, в результате чего повышается вероятность того, что информационная система готова к эксплуатации $P_{\text{гэ}}$, определяемая в предположении того, что в системе используется V элементов с номерами $v=1,\ldots,V$ ($V-1$из которых являются резервирующими элементами) при вероятности готовности v-го элемента к эксплуатации в$P_{\text{гэ}v}$, следующим образом (отказы коммутирующих элементов для простоты не рассматриваем):

$$P_{\text{гэ}} = 1 - \prod_{v=1}^{V} (1 - P_{\text{гэ}v})$$

Эффект достигается за счет того, что при отказе одного из зарезервированных элементов информационная система продолжает свое функционирование.

В качестве резервирующих элементов, используемых с целью увеличения надежности (отказоустойчивости) функционирования информационной системы, могут применяться как полностью одинаковые(в этом случае для них будет совпадать значение характеристики $P_{\text{гэ}v}$), так и различные (при соответствующем различии значений характеристики $P_{\text{гэ}v}$) технические средства.

Это обусловливается тем, что в общем случае отказы резервируемого и резервирующих элементов можно рассматривать как независимые события (возможность отказов коммутирующих и переключающих элементов, используемых для создания схемы резервирования, не рассматриваем). Как следствие, в качестве резервирующих элементов (используемых)можно применять как полностью одинаковые с резервируемыми, так и отличные технические средства.Важным здесь является исключительно влияние характеристики резервирующего элемента $P_{\text{гэ}v}$ на характеристику $P_{\text{гэ}}$ информационной системы в целом.

Замечание. В данном исследовании мы не рассматриваем все многообразие возможных постановок задач и методов резервирования элементов информационной системы[14]. Нам достаточно определить и сравнить между собою ключевые возможности подходов к резервированию при решении задач повышения уровня надежности функционирования и уровня информационной безопасности информационной системы.

3.3. Задачи резервирования элементов системы, решаемые с целью повышения уровня безопасности информационной системы

Как ранее отмечали, информационная безопасность имеет несколько ключевых характеристик, сопоставимо важных при решении задач повышения уровня информационной безопасности систем. К характеристикам информационной безопасности относятся: защита от нарушения конфиденциальности информации (защита от ее хищения), защита от нарушения целостности информации (защита от ее несанкционированной модификации), защита от нарушения доступности информации. Для выявления соответствующих противоречий нам будет достаточно рассмотреть две из них: защита от нарушения конфиденциальности информации и защита от нарушения доступности информации.

Поскольку задачу повышения уровня надежности функционирования информационной системы также отчасти можно рассматривать в контексте обеспечения доступности информации, правда, отказ характеристики информационной безопасности в данном случае обусловливается реализацией успешной атаки (а не отказом оборудования), направленной на уничтожение обрабатываемой в информационной системе информации (либо иных ресурсов, приводящих к невозможности получения доступа к информации), исследование вопросов резервирования элементов информационной системы начнем применительно именно к характеристике нарушения доступности информации.

3.3.1. Задача резервирования элементов системы, решаемая для защиты от нарушения доступности обрабатываемой в информационной системе информации

Повышение уровня защиты от нарушения доступности информации резервированием возможно и достигается в том случае, когда применяются резервирующие элементы, не зависимые между собою и с резервируемым элементом по угрозам атак (по потенциально возможным атакам), т.е. в качестве зарезервированных элементов применяются различные технические средства.

Докажем данное утверждение. Пусть каждый из *V* зарезервированных элементов с номерами *v=1,…,V* может быть определен соответствующей характеристикой –вероятностью того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных угроз атак, образующих угрозу безопасности элемента информационной системы,$P_{0\text{Уэ}v}$.

В случае если все угрозы атак для всех V резервируемых элементов системы не зависимы – различны, то вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных угроз атак,$P_{0\text{Уэ}V}$ может быть определена следующим образом:

$$P_{0\text{Уэ}V} = 1 - \prod_{\text{v}=1}^{\text{V}} (1 - P_{0\text{Уэ}v})$$

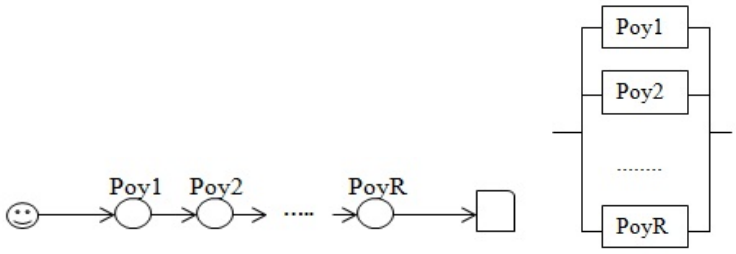
В случае если с целью повышения уровня защиты от нарушения доступности информации резервированием применяются резервирующие элементы, полностью зависимые между собою и с резервируемым элементом по угрозам атак (по потенциально возможным атакам), т.е. в качестве зарезервированных элементов применяются одинаковые технические средства, резервирование элементов не реализуется. Это обусловливается следующим. В случае если все угрозы атак для всех *V* зарезервированных элементов системы зависимы – угрозы атак соответствующим образом совпадают для всех элементов, то вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных угроз атак,$P_{0\text{Уэ}V}$ с учетом того, что $P_{0\text{Уэ}v=1} = P_{0\text{Уэ}v=2} = \cdots = P_{0\text{Уэ}v=V}$, может быть определена следующим образом:

$$P_{0\text{Уэ}V} = P_{0\text{Уэ}v}$$

Резервирование элементов информационной системы в части повышения уровня безопасности можно интерпретировать соответствующей схемой резервирования в отношении угроз атак, при этом можно говорить о том, что задача резервирования элементов информационной системы сводится к задаче резервирования по угрозам атак.

Рассмотрим модель резервирования по угрозам атак. Для наглядности (простоты представления) предположим, что каждый из *R* зарезервированных элементов информационной системы подвержен только одной угрозе атаки. Если угрозы атак всех зарезервированных элементов системы уникальны (не зависимы) и характеризуются $P_{0\text{у}r}$, *r=1,....,R*(для

соответствующихRзарезервированных элементов), вероятностью того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможныхугрозатаки, то для осуществления успешной атаки на информационную систему в целом должна быть осуществлена успешная атака на каждый из зарезервированных элементов (реализованы угрозы информационной безопасности всех резервирующих элементов)– выведены из строя (рассматриваем характеристику доступности информации) все зарезервированные элементы информационной системы. В результате сказанного получаем орграф, см. рис.26, "взвешенными" (значениями P_{0yr} ,*r=1,....,R*) вершинами которого выступают вершины угроз атак зарезервированных элементов, и соответствующую ему схему параллельного резервирования.



а. Орграф угроз атак б. Схема параллельного резервирования

Рис.26. Модель резервирования по угрозам атак при защитеот нарушения доступности информации

Обозначим характеристику некой произвольной угрозы атаки как P_{0y} (пусть рассматриваем угрозу подобной атаки на элемент системы *v=1*), для остальных элементов системы *v=2,...,V* обозначаем соответствующую характеристику, как и прежде,$P_{0Уэv}$.В данных предположениях соответствующая характеристика зарезервированной информационной системы$P_{0УэV}$может быть представлена следующим образом:

$$P_{0УэV} = 1 - (1 - P_{0y}) \prod_{v=2}^{V} (1 - P_{0Уэv})$$

Если же одна и та же угроза атаки с характеристикойP_{0y} совпадает, например, для элементов *v=1, v=2, v=3* из *V* зарезервированных элементов, то для $P_{0УэV}$уже получаем:

$$P_{0УэV} = 1 - (1 - P_{0y}) \prod_{v=4}^{V} (1 - P_{0Уэv})$$

В пределе – угроза атаки совпадает для всех зарезервированных элементовV, имеем:

$$P_{0УэV} = P_{0y},$$

т.е. в данном случае (применительно к подобной угрозе атаки) все угрозы атак зарезервированного и резервирующих элементов информационной системы зависимы – задача резервирования не решается.

Следствия.

1. Задача резервирования элементов информационной системы применительно к решению задач повышения уровня информационной безопасности информационных систем в части защиты от нарушения доступности информации сводится к задаче резервирования угроз атак на элемент информационной системы посредством резервирования данного элемента элементом (элементами), характеризуемым отличными(независимыми) угрозами атак.

2. При полном совпадении резервируемого и резервирующего элементов информационной системы задача резервирования элементов информационной системы с целью повышения уровня информационной безопасности в части защиты от нарушения доступности информации резервированием не решается, поскольку в данном случае не реализуется резервирования по угрозам атак.

Сказанное позволяет ввести понятие и количественную оценку актуальности угрозы атаки, но уже на зарезервированную информационную систему (на зарезервированный элемент информационной системы).

Под количественной оценкой актуальности угрозы атаки на зарезервированную информационную систему (на зарезервированный элемент информационной системы) будем понимать значение вероятности готовности к безопасной эксплуатации зарезервированной информационной системы в отношении угрозы этой атаки$P_{0\text{Уэ}v}$. Естественно, что к наиболее актуальным угрозам атак при результате резервирования элементов информационной системы будут отнесены незарезервированные угрозы атак – угрозы атак, актуальные и для резервируемого, и для резервирующих элементов информационной системы. Именно в отношении подобных угроз атак при резервировании элементов информационной системыв первую очередь потребуется применение средств защиты, направленных на повышение значения характеристики $P_{0\text{Уэ}v}$.

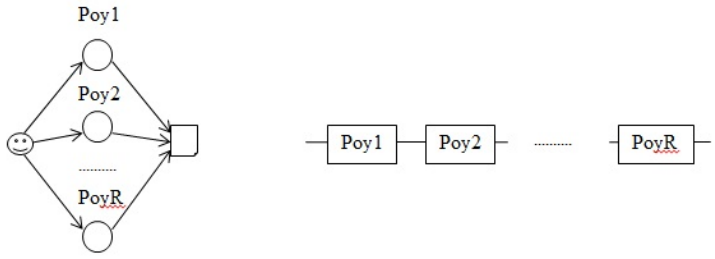
Следствие. Задачи защиты от нарушения доступности информации, которое может быть вызвано как отказом элемента системы, так и реализацией атаки на этот элемент нарушителем безопасности, могут решаться в комплексе, при этом можно говорить о решении задачи повышения уровня интегрированной информационно-эксплуатационной безопасности информационных систем в части данных характеристик. При этом задача повышения уровня интегрированной информационно-эксплуатационной безопасности информационных систем позволяет определитьи вполне определенную постановку задачи повышения уровня надежности (отказоустойчивости) информационных систем, предполагающую обеспечение

максимального различия технических средств, используемых в качестве резервируемого и резервирующих элементов, что обеспечивает их максимальное различие по угрозам атак.

3.3.2. Задача резервирования элементов системы, решаемая для защиты от нарушения конфиденциальности обрабатываемой в информационной системе информации

Нарушение характеристики конфиденциальности информации также может быть реализовано в результате реализации нарушителем атаки на информационную систему, но уже с целью хищения обрабатываемой в ней информации.

Рассмотрим модель резервирования по угрозам атак при решении данной задачи резервирования. Опять же для наглядности (простоты представления) предположим, что каждый из *R* зарезервированных элементов информационной системы подвержен только одной угрозе атаки. Если угрозы атак всех зарезервированных элементов системы уникальны (не зависимы) и характеризуются P_{0yr}, $r=1,....,R$(для соответствующих*R*зарезервированных элементов),вероятностью того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможной угрозы атаки, то для осуществления успешной атаки на информационную систему в целом достаточно реализации успешной атаки на любой из зарезервированных элементов (в этом случае обрабатываемая информация будет похищена). В результате сказанного получаем орграф, см. рис.27, взвешенными вершинами которого выступают вершины угроз атак зарезервированных элементов, и соответствующую ему схему резервирования, но уже последовательного резервирования.



а. Орграф угроз атак б. Схема последовательного резервирования

Рис.27. Модель резервирования по угрозам атак при защите от нарушения конфиденциальности информации

Повышение уровня защищенности информационной системы от нарушения конфиденциальности информации резервированием принципиально невозможно, поскольку в данном случае невозможно резервирование по угрозам атак.

Докажем это утверждение.Пусть каждый из *V* зарезервированных элементов с номерами *v=1,…,V*может быть представлен соответствующей характеристикой – вероятностью того, что

информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак, образующих угрозу безопасности элемента информационной системы,$P_{0\text{Уэ}v}$.

В случае если все угрозы атак в V резервируемых элементах системы зависимы (полностью совпадают), при этом для хищения информации достаточно осуществить успешную атаку на любой из V зарезервированных элементов, то вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак,$P_{0\text{Уэ}V}$с учетом того, что $P_{0\text{Уэ}v=1} = P_{0\text{Уэ}v=2} = \cdots = P_{0\text{Уэ}v=V}$, в данных предположениях может быть определена следующим образом:

$$P_{0\text{Уэ}V} = P_{0\text{Уэ}v}$$

В случае же если все угрозы атак в V зарезервированных элементах системы независимы (соответствующим образом различаются во всех элементах), при этом для хищения информации достаточно осуществить успешную атаку на любой из V зарезервированных элементов, то вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак,$P_{0\text{Уэ}V}$:

$$P_{0\text{Уэ}V} = \prod_{\text{v}=1}^{\text{V}} P_{0\text{Уэ}v}$$

Как видим, попытка решения задачи повышения уровня безопасности информационной системы в части защиты от нарушения конфиденциальности информации резервированиемможет приводить лишь к снижению уровня безопасности. Причем, как ранее отмечали, повышение уровня защиты от нарушения доступности информации резервированием возможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собою и с резервируемым элементом по угрозам атак (в случае реализации резервирования по угрозам атак), но именно при этих условиях снижается уровень безопасности информационной системы в части защиты от нарушения конфиденциальности информации.

Следствия.

1. Резервирование элементов информационной системы по угрозам атак не позволяет повысить уровень информационной безопасности системы в части защиты от нарушения конфиденциальности информации.

2. Реализация резервирования элементов информационной системы по угрозам атак приводит к снижению уровня информационной безопасности системы в части защиты от нарушения конфиденциальности информации.

Выводы.

1. Применение известных методов резервирования элементов информационных систем в теории информационной безопасности связано с фундаментальным противоречием, состоящим в том, что задачи повышения уровня безопасности информационной системы в части защиты от нарушения доступности информации и повышения уровня безопасности информационной системы в части защиты от нарушения конфиденциальности информации, не могут решаться в комплексе,поскольку улучшение одной из этих характеристик информационной безопасности в результате реализации резервирования по угрозам атак элементов информационной системы приводит к ухудшению другой характеристики, что недопустимо ввиду сопоставимой важности данных характеристик для современных информационных систем. В этом смысле известные методы резервирования не могут эффективно использоваться в информационной безопасности. Данное противоречие методов резервирования в информационной безопасности может быть отнесены к фундаментальным ввиду того, что оно никак не связано с какими-либо характеристиками защищаемых информационных систем, используемым в них оборудованием, программными средствами и т.д. Данные противоречия обусловливаются собственно постановкой задачи резервирования элементов информационных систем в области информационной безопасности как задачи резервирования угроз атак в элементах информационных систем.

2. Эффективное решение резервированием задачи повышения интегрированной информационно-эксплуатационной безопасности информационных систем известными из теории надежности методами резервирования возможно только в части защиты от нарушения доступности информации, которое может быть вызвано как отказом элемента системы, так и реализацией атаки на элемент системы. Однако при решении этой задачи резервирования ухудшается важнейшая характеристика информационной безопасности информационной системы – характеристика конфиденциальности обрабатываемой информации.

3. Поскольку в современных информационных системах задачи повышения уровня надежности и информационной безопасности должны решаться в комплексе, причем в части информационной безопасности в комплексе должны решаться задачи повышения уровня конфиденциальности и доступности информации, а известные из теории надежности методы резервирования для этого неэффективны, необходима разработка новых, принципиально иных подходов к резервированию элементов информационных систем, позволяющих учесть выявленные фундаментальные противоречия методов резервирования в области информационной безопасности.

3.4. Метод резервирования с разделением обработки информации между элементами системы

Проведенное выше исследование показало, что резервирование для решения задачи повышения уровня конфиденциальности обрабатываемой в информационной системе информации с использованием известных из теории надежности методов резервирования не может использоваться в принципе, что, прежде всего, и делает неэффективным применение известных методов резервирования элементов информационных систем в области информационной безопасности.

Рассмотрим задачу повышения уровня безопасности в части обеспечения конфиденциальности информации с позиций оценки риска потенциальных потерь [22]. Риск потенциальных потерь $R_{C_{\text{Уинф}}}$ применительно к угрозе информационной безопасности информационной системы (характеристика угрозы информационной безопасности информационной системы $P_{0\text{УэУ}}$) в простейшем случае (без учета изменения данной характеристики в процессе эксплуатации информационной системы, о чем говорили ранее) можно оценить следующим образом:

$$R_{C_{\text{Уинф}}} = C_{\text{инф}} (1 - P_{0\text{УэУ}})$$

Характеристика потерь $C_{\text{инф}}$ зависит от объема похищенной информации [13]. Введем характеристику удельной стоимости $C_{\text{уинф}}$ единицы информации. Исходя из того, что в информационной системе обрабатывается N единиц информации, характеризуемых удельной стоимостью $C_{\text{уинф}}$, величину потерь, обусловливаемых хищением обрабатываемой в информационной системе информации, можем представить следующим образом:

$$C_{\text{инф}} = C_{\text{уинф}} N$$

С учетом этого задача повышения резервированием элементов информационной системы уровня информационной безопасности в части защиты от нарушения конфиденциальности информации может рассматриваться как задача снижения потерь от реализации успешной атаки на элемент информационной системы при разделении (не каком-либо функциональном, исключительно по объему) между зарезервированными элементами обрабатываемой информации. Задача резервирования в данном случае предполагает разделение хранения и обработки информации между V зарезервированными элементами информационной системы при равном распределении между V элементами объемов обрабатываемой информации: на каждом из них будет сконцентрирована информация, стоимостью $C_{\text{инф}v}$:

$$C_{\text{инф}v} = C_{\text{уинф}} N/V$$

Следовательно, потери от реализации успешной атаки на один из зарезервированных элементов информационной системы составят $C_{\text{инф}v}$, что снизит потери от успешной атаки на элемент информационной системы в V раз.

Назовем подобный метод резервирования "методом резервирования с разделением обработки информации между элементами системы".

Повышение уровня безопасности информационной системы в частихарактеристики нарушения конфиденциальности информации методом резервирования с разделением обработки информации между элементами системывозможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собою и с резервируемым элементом по угрозам атак (по потенциально возможным атакам).

Докажем это утверждение.В случае если все угрозы атак в Vзарезервированных элементах системы зависимы – соответствующим образом полностью совпадают, т.е. одна и та же атака может быть реализована на все V зарезервированных элемента (резервирования по угрозам атак не реализовано), риск потерь от реализации угрозы атаки на элемент системы (характеристика угрозы атаки на любой элемент системы $P_{0\text{Уэ}v}$) $R_{C_{\text{Уинф}}}$ рассчитывается следующим образом:

$$R_{C_{\text{Уинф}}} = C_{\text{инф}}\,(1 - P_{0\text{Уэ}v})$$

В случае же если все угрозы атак в V резервируемых элементах системы не зависимы – соответствующим образом различаются во всех элементах (зарезервированы), одна и та же атака может быть реализована только на один из Vзарезервированный элемент, для $R_{C_{\text{Уинф}}}$имеем:

$$R_{C_{\text{Уинф}}} = C_{\text{инф}}\,(1 - P_{0\text{Уэ}v})/V$$

Представленные выше формулы для альтернативных рассмотренных случаев доказывают, что повышение уровня безопасности от нарушения конфиденциальности информации резервированием возможно и достигается только в том случае, когда применяются резервирующие элементы, не зависимые между собою и с резервируемым элементом по угрозам атак (по потенциально возможным атакам); при этом резервирование элемента полностью идентичными по угрозам атак элементами не может использоваться в информационной системе с целью повышения уровня безопасности от нарушения конфиденциальности информации.

Применение метода резервирования с разделением обработки информации между элементами системы в случае реализации резервирования по угрозам атак (используются различные технические средства для построения зарезервированных элементов информационной системы), позволяющего снизить риск потенциальных потерь от реализации

успешной атаки на информационную систему (в V *раз)*,приводит к увеличению риска частичных потерь обрабатываемой в информационной системе информации –риска потерьинформациив объеме, обрабатываемом одним из зарезервированных элементов системы.

Сказанное подтверждается следующим. Ранее мы показали, что в случае, если все угрозы атак в V зарезервированных элементах системы независимы (зарезервированы) – соответствующим образом различаются во всех зарезервированных элементах, для хищения информации в объеме, обрабатываемом одним из зарезервированных элементов системы, достаточно осуществить успешную атаку на любой из V зарезервированных элементов. Вероятность того, что в этом случае информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак,$P_{0\text{Уэ}V}$:

$$P_{0\text{Уэ}V} = \prod_{\text{v}=1}^{\text{V}} P_{0\text{Уэ}v}$$

В случае же если все угрозы атак в V резервируемых элементах системы зависимы – полностью совпадают (не зарезервированы), при этом для хищения информации в объеме, обрабатываемом одним из зарезервированных элементов системы, достаточно осуществить успешную атаку на любой из V зарезервированных элементов, вероятность того, что информационная система готова к безопасной эксплуатации в отношении потенциально возможных атак, $P_{0\text{Уэ}V}$ с учетом того, что $P_{0\text{Уэ}v=1} = P_{0\text{Уэ}v=2} = \cdots = P_{0\text{Уэ}v=V}$, может быть определена следующим образом:

$$P_{0\text{Уэ}V} = P_{0\text{Уэ}v}$$

Однако в этом случаерезервирования по угрозам атак не будет реализовано, поскольку одна и та же успешная атака может быть осуществлена на всеV зарезервированных элемента системы. В этом случае уже следует говорить о риске хищения всей обрабатываемой в информационной системе информации и о соответствующем для этого случае риске потерь, связанным с хищением информации стоимостью $C_{\text{инф}}$.

Следствие. Данное противоречие – снижение риска хищения информации обрабатываемой в информационной системе в полном объеме при одновременном увеличении риска хищения информации в объеме, обрабатываемом одним из зарезервированных элементов системы, можно считать принципиальным противоречием метода резервирования с разделением обработки информации между элементами системы.

Это крайне важное противоречие данного метода резервирования в обязательном порядке должно учитываться при разработке требований к характеристикам и параметрам средств защиты информации, реализуемых (при необходимости) в резервируемых элементах информационной системы.

Выводы.

1. Метод резервирования с разделением обработки информации между элементами системы позволяет повышать резервированием элементов информационной системы уровень информационной безопасности как в части защиты от нарушения доступности информации, так и в части защиты от нарушения конфиденциальности информации. Это обусловливается тем, что обе эти задачи резервирования решаются в том случае, когда применяются резервирующие элементы, не зависимые между собою и с резервируемым элементом по угрозам атак (реализуется резервирование по угрозам атак). Т.е. требования к решению данных задач повышения уровня информационной безопасности системы не противоречат друг другу.

2. Метод резервирования с разделением обработки информации между элементами системы может применяться для решения задачи повышения уровня интегрированной информационно-эксплуатационной безопасности. Это обусловливается тем, что обе эти задачи резервирования, реализуемого и с целью повышения уровня надежности функционирования системы, и с целью повышения уровня ее информационной безопасности, решаются в том случае, когда применяются резервирующие элементы, не зависимые между собою и с резервируемым элементом по угрозам атак (реализуется резервирование по угрозам атак). Т.е. требования к решению данных задач повышения уровня интегрированной информационно-эксплуатационной безопасности не противоречат друг другу.

Однако метод резервирования с разделением обработки информации между элементами системы не позволяет решать задачу повышения уровня надежности функционирования информационной системы в полном объеме, что следует из того, что при отказе зарезервированного элемента системы в информационной системе становится невозможной обработка информации, хранящейся в нем и обрабатываемой этим элементом системы, при возможности продолжения обработки информации иными элементами системы.

Следствие. Этот недостаток резервирования также может быть отнесен к принципиальным недостаткам метода резервирования с разделением обработки информации между элементами системы. Данный недостаток делает неэффективным использование метода резервирования с разделением обработки информации между элементами системы для решения отдельно взятой задачи повышения уровня безопасности информационной системы в части обеспечения доступности обрабатываемой информации.

Вывод.

Метод резервирования с разделением обработки информации между элементами системы принципиально может применяться для решения задачи повышения уровня интегрированной информационно-эксплуатационной безопасности, но ввиду его

принципиальных недостатков данный метод должен рассматриватьсялишь как некое компромиссное решение.

ЗАКЛЮЧЕНИЕ

В данном учебном пособии изложен математический аппарат, который может быть применен для формального проектирования систем защиты информационных систем и для оценки их эффективности. К основным преимуществам рассмотренных методов моделирования и проектирования систем защиты информационных систем можно отнести то, что для решения рассматриваемых задач не требуется использование каких-либо экспертных оценок – при моделировании используются лишь стохастические значения параметров безопасности уязвимостей (угроз уязвимостей), в отношении которых имеется вся необходимая статистика. Поясним, почему это так важно.

Для этого, прежде всего, ответим на вопрос: при каких условиях и с какой целью используются экспертные оценки? Ответ крайне прост: в том случае, когда разработчикам соответствующих математических моделей не удается математически смоделировать какие-либо параметры или характеристики системы, цель также очевидна – хоть как-то количественно задать значения требуемых параметров/характеристик. Другими словами, использование экспертных оценок – это от «безысходности» – от невозможности решения требуемых задач математическими методами. На самом деле, при этом одна неопределенность подменяется иной, причем порою возникает резонно вопрос: что сложнее экспертно оценить – некое моделируемое совокупное качество системы либо некое ее локальное качество, к чему сводится экспертное оценивание разработанной математической моделью?

Ключевой недостаток использования экспертных оценок в математических моделях обусловливается принципиальной невозможностью какого-либо оценивания адекватности получаемых в итоге результатов, т.е. проектные решения должны приниматься, исходя из принципиальной невозможности ответа на вопрос:на сколько результаты моделирования соответствуют действительности? Дело в том, что основную погрешность в подобных эвристически-математических (математическими их назвать никак нельзя) методах моделирования несет в себе именноэкспертное задание значений требуемыхпараметров/характеристик, причем каким-либо образом оценить подобную погрешность не представляется возможным. Исходить же при моделировании из концепции «абсолютно квалифицированного эксперта» вряд ли разумно. Где ж такого найти, особенно в такой сложной области знаний, как информационная безопасность?

К слову сказать, на практике методы моделирования, предполагающие экспертное оценивание каких-либо параметров/характеристик системы, могут и осознано эксплуатироваться недобросовестными проектировщиками систем защиты информационных систем. Ввиду того, что современная концепция построения системы защиты информационной системы предполагает реализацию защиты от актуальных угроз, к которым экспертным путем относятся соответствующие угрозы из набора потенциально возможных угроз [2,3], экспертным путем ту или иную угрозу при проектировании системы защиты можно и не отнести к актуальным для какой-либо информационной системы, ведь нет единой формальной количественной оценки актуальности угрозы – все основывается на некой оценке некоего эксперта, а мнения различных экспертов могут сильно отличаться либо вообще быть противоположными, снизив тем самым затраты на реализацию защиты, естественно, снизив тем самым и эффективность защиты. При наличии же формальной количественной оценки актуальности угрозы подобное становится уже невозможным.

Важнейшим результатом исследований, приведенном в данном учебном пособии, является обоснование невозможности эффективного использования известных из теории надежности методов резервирования элементов информационной системы для решения как задач повышения уровня информационной безопасности, так и задачи повышения уровня интегрированной информационно-эксплуатационной безопасности информационной системы. В качестве компромиссного решения рассмотрен метод резервирования с разделением обработки информации между элементами системы. Вместе с тем, выявленные существенные недостатки данного метода резервирования иллюстрируют необходимость дальнейшего исследования этих ключевых вопросов (вопросов резервирования элементов) построения защищенных информационных систем.

Однако одно дело – при проектировании определить то, какие задачи защиты должны решаться системой защиты, сформировать требования кзначениям параметров и характеристик системы защиты, и совсем другое дело – определить то, как должны решаться эти задачи: как собственно реализовать эффективную защиту информации на практике, как обеспечить корректность реализации защиты – сформировать и реализовать такие требования к системе защиты, выполнение которых позволит построить безопасную систему, исходя из того, что системой защиты должны нивелироваться актуальные угрозы уязвимостей информационной системы, либо предотвращаться последствия реализации соответствующих угроз уязвимостей (в учебном пособии дано обоснование тому, что именно этими методами может быть реализована эффективная защита современных информационных систем). Эти и иные вопросы проектирования систем защиты информационных систем, но уже в части разработки методов

защиты, исследования возможностей их практического использования, обоснования требований к построению безопасной системы при их применении, изложены в учебном пособии [28].

ЛИТЕРАТУРА

1.ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации, 2009.

2.Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Нормативный документ ФСТЭК России, 2008.

3.Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. N 17.

4. Белов Е.Б, Лось В.П., Мещеряков Р.В., Шелупанов А.А.. Основы информационной безопасности. М.: Горячая линия - Телеком, 2006.

5. Богатырев В.А., Богатырев С.В., Богатырев А.В. Надежность кластерных вычислительных систем с дублированными связями серверов и устройств хранения//Информационные технологии.- 2013. № 2. С. 27-32.

6. Вентцель Е.С. Исследование операций. - М.: Советское радио, 1972.

7.Королев В.Ю., Бенинг В.Е., Шоргин С.Я. Математические основы теории риска. М.: Физматлит, 2011.

8.Корт С.С. Теоретические основы защиты информации: Учебное пособие - М.: Гелиос АРВ, 2004.

9.Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. - К.:МК-Пресс, 2006.

10.Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. - М.:Горячая линия - Телеком, 2004.

11. Маркина Т.А., Щеглов А.Ю. Метод защиты от атак типа drive-by загрузка // Известия ВУЗов. Приборостроение, 2014. - № 4. - С. 15-20.

12.Мельников В.В. Безопасность информации в автоматизированных системах. -М.: Финансы и статистика, 2003.

13.Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. - М.: Компания АйТи; ДМК Пресс, 2004.

14.Половко А.М., Гуров С.В. Основы теории надежности. - СПб.: БХВ-Петербург. - 2006.

15. Росенко А.П. Внутренние угрозы безопасности конфиденциальной информации: Методология и теоретическое исследование. - М: Красанд, 2010.

16.Саати Т. Элементы теории массового обслуживания и ее приложения. – М.: Изд. «СОВЕТСКОЕ РАДИО», 1965.

17. Саркисян С.А и др. Теория прогнозирования и принятия решений. – М.: Высшая школа. – 1977.

18. Соколов. А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. - М.: ДМК Пресс, 2002.

19.Шапкин А.С., Шапкин В.А.. Теория риска и моделирование рисковых ситуаций. - М.: Дашков и К, 2005.

20.Шеннон К.Е. Математическая теория связи // Работы по теории информации и кибернетике, пер. с англ., М., 1963, с. 243-332.

21.Щеглов К.А., Щеглов А.Ю. Защита от атак на уязвимости приложений. Модели контроля доступа // Вопросы защиты информации. - 2013. - Вып. 101. - № 2. - С. 36-43.

22.Щеглов К.А., Щеглов А.Ю. Эксплуатационные характеристики риска нарушений безопасности информационной системы // Научно-технический вестник информационных технологий, механики и оптики. - 2014. - №1(89). - С.129-139.

23.Щеглов К.А., Щеглов А.Ю. Математические модели эксплуатационной информационной безопасности // Вопросы защиты информации. - 2014. - Вып. 106. - № 3. - С. 52-65.

24. Щеглов К.А., Щеглов А.Ю. Защита от вредоносных программ методом контроля доступа к создаваемым файловым объектам//Вестник компьютерных и информационных технологий. - 2012. - № 8. - С. 46-51.

25. Щеглов К.А., Щеглов А.Ю. Защита от атак на повышение привилегий // Вестник компьютерных и информационных технологий. - 2015. - № 1. - С. 36-42.

26. Щеглов К.А., Щеглов А.Ю. Защита от атак на уязвимости приложений // Информационные технологии. - 2014. - № 9. - С. 34-39.

27. Щеглов К.А., Щеглов А.Ю. Контроль доступа к статичным файловым объектам // Вопросы защиты информации. - 2012. - Вып. 97. - № 2. - С. 12-20.

28.Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем. Учебное пособие. – СПб: Университет ИТМО, 2014. – 95 с.

29.Итоги 2013: угрозы и эксплуатация Windows[Электронный ресурс]. Режим доступа http://www.habrahabr.ru/company/eset/blog/209694/, свободный (02.04.2014).

30.Отчет по уязвимостям 20.02-26.02 2012 [Электронный ресурс]. Режим доступа: URL:/ http://www.securitylab.ru/vulnerability/reports/420676.php, свободный (02.04.2014).

31.Полное руководство по общему стандарту оценки уязвимостей версии 2. Часть первая. Группы метрик [Электронный ресурс]. Режим доступа: http:// www.securitylab.ru/analytics/355336.php , свободный (02.04.2014).

32.Шабанов И. Антивирусныевендоры ищут выход из технологического тупика. Аналитический центр Anti-Malware.ru [Электронный ресурс]. Режим доступа: http://www.anti-malware.ru/antivirus_trends, свободный (02.04.2014).

33.Эксперты: трояны по-прежнему остаются самым популярным вредоносным ПО [Электронный ресурс]. Режим доступа: http://www.itsec.ru/newstext.php?news_id=100297, свободный (02.04.2014).

34.ApplicationSecurityInc.VulnerabilityDisclosurePolicy[Электронныйресурс]. Режимдоступа: http://www.appsecinc.com/aboutus/vulndisclosepolicy, свободный (02.04.2014).

35.CERT/CC Vulnerability Disclosure Policy [Электронныйресурс]. Режим доступа: http://http://www.cert.org/kb/vul_disclosure.html, свободный (02.04.2014).

36.FIRST [Электронный ресурс]. Режим доступа: http://www.first.org, свободный (02.04.2014).

37.Microsoft Security Response Center Security Bulletin Severity Rating System [Электронныйресурс]. Режим доступа: http://www.microsoft.com/technet/security/ bulletin/rating.mspx, свободный (02.04.2014).

38.KasperskySecurityBulletin. Основная статистика за 2011 год [Электронный ресурс]. Режим доступа: http://http://www.securelist.com/ru/analysis/208050741/rss/analysis, свободный (02.04.2014).

39.SANS Critical Vulnerability Analysis Archive [Электронныйресурс]. Режим доступа: http://www.sans.org/newsletters/cva/ , свободный (02.04.2014).

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

О кафедре

Кафедра вычислительной техники Университета ИТМО создана в 1937 году и является одной из старейших и авторитетнейших научно-педагогических школ России.

Первоначально кафедра называлась кафедрой математических и счетно-решающих приборов и устройств и занималась разработкой электромеханических вычислительных устройств и приборов управления. Свое нынешнее название кафедра получила в 1963 году.

Кафедра вычислительной техники является одной из крупнейших в университете, на которой работают высококвалифицированные специалисты, в том числе 7 профессоров и 14 доцентов.

Кафедра имеет 4 компьютерных класса, объединяющих более 70 компьютеров в локальную вычислительную сеть кафедры и обеспечивающих доступ студентов ко всем информационным ресурсам кафедры и выход в Интернет. Кроме того, на кафедре имеются учебные и научно-исследовательские лаборатории по вычислительной технике, в которых работают студенты кафедры.

Чему мы учим

Традиционно на кафедре вычислительной техники Университета ИТМО основной упор в подготовке специалистов делается на фундаментальную базовую подготовку в рамках общепрофессиональных и специальных дисциплин, охватывающих наиболее важные разделы вычислительной техники: функциональная схемотехника и микропроцессорная техника, алгоритмизация и программирование, информационные системы и базы данных, мультимедиа технологии, вычислительные сети и средства телекоммуникации, защита информации и информационная безопасность. В то же время, кафедра предоставляет студентам старших

курсов возможность специализироваться в более узких профессиональных областях в соответствии с их интересами.

Специализации на выбор

Кафедра вычислительной техники Университета ИТМО ведёт подготовку специалистов высшей квалификации в соответствии с Государственными образовательными стандартами 3-го поколения (ГОС-3) по двум направлениям:

09.04.01 «Информатика и вычислительная техника» (*профиль подготовки «Вычислительные машины, комплексы, системы и сети»*);
09.04.04 «Программная инженерия» (*профиль подготовки «Разработка программно-информационных систем»*);
с присвоением степени (квалификации) бакалавр (срок обучения – 4 года).

Прием абитуриентов на указанные направления подготовки бакалавров осуществляется в соответствии с общими Правилами приема в Университет ИТМО.

Студенты, успешно завершившие обучение и получившие диплом *бакалавра*, могут продолжить обучение в магистратуре кафедры (срок обучения – 2 года) по следующим магистерским программам:

- «Безопасность вычислительных систем и сетей» – руководитель д.т.н. профессор Щеглов Андрей Юрьевич;
- «Вычислительные системы и сети»– руководитель д.т.н. профессор АлиевТауфикИзмайлович;
- «Информационно-вычислительные системы»– руководитель д.т.н. профессор АлиевТауфикИзмайлович;
- «Интеллектуальные информационные системы» – руководитель д.т.н. профессор Тропченко Александр Ювенальевич;
- «Проектирование встроенных вычислительных систем» – руководитель д.т.н. профессор Платунов Алексей Евгеньевич;
- «Системотехника интегральных вычислителей. Системы на кристалле» – руководитель д.т.н. профессор Платунов Алексей Евгеньевич;
- «Сетевые встроенные системы» - руководитель д.т.н. профессор Платунов Алексей Евгеньевич;
- «Технологии компьютерной визуализации» (совместно с базовой кафедрой Института Прикладной математики им. М.В. Келдыша) – руководитель д.т.н. профессор Палташев Тимур Турсунович.

В магистратуру на конкурсной основе принимаются выпускники других вузов, имеющие диплом бакалавра.

На кафедре вычислительной техники Университета ИТМО в рамках аспирантуры и докторантуры осуществляется подготовка научных кадров по следующим *специальностям*:

- 05.13.05 – Элементы и устройства вычислительной техники и систем управления (технические науки);
- 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей (технические науки);
- 05.13.12 – Системы автоматизации проектирования (приборостроение) (технические науки);
- 05.13.15 – Вычислительные машины, комплексы и компьютерные сети (технические науки);
- 05.13.17 – Теоретические основы информатики (технические науки);
- 05.13.18 – Математическое моделирование, численные методы и комплексы программ (технические науки);
- 05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки).

Щеглов Андрей Юрьевич

Модели, методы и средства контроля доступа к ресурсам вычислительных систем

Учебное пособие

В авторской редакции

Редакционно-издательский отдел Университет ИТМО

Зав. РИО Н.Ф. Гусарова

Подписано к печати …

Заказ №

Тираж

Отпечатано на ризографе

Редакционно-издательский отдел

Университета ИТМО

197101, Санкт-Петербург, Кронверкский пр., 49