

Министерство образования и науки Российской Федерации
Ярославский государственный университет им. П. Г. Демидова

Кафедра компьютерной безопасности и
математических методов обработки информации

Техническое противодействие компьютерной разведке

Часть 1

Учебно-методическое пособие

Ярославль
ЯрГУ
2017

УДК 004.732.056(075.8)
ББК 32.973.2-018.2я73
Т38

*Рекомендовано
Редакционно-издательским советом университета
в качестве учебного издания. План 2017 года*

Рецензент:

Дурнев В.Г. – доктор физико-математических наук, профессор,
кафедра компьютерной безопасности и математических методов
обработки информации, Ярославский государственный
университет им. П.Г. Демидова»

Составитель
Ю. И. Ушаков

Техническое противодействие компьютерной разведке :
Т38 учебно-методическое пособие. Ч. 1 / сост. Ю. И. Ушаков ; Яросл.
гос. ун-т им. П. Г. Демидова. – Ярославль : ЯрГУ, 2017. – 170 с.

В учебно-методическом пособии рассмотрены принятые в Российской Федерации современные технические меры и методы противодействия компьютерной разведке как неотъемлемой части специальных информационных операций и атак. Рассматриваются цели, роли и способы проведения современной компьютерной разведки, а также основания, формы, методы и приемы организационного и технического противодействия ей в условиях иностранного технического доминирования в телекоммуникационных технологиях и сетях связи.

УДК 004.732.056(075.8)
ББК 32.973.2-018.2я73

© ЯрГУ, 2017

Введение

Реалии современного исторического этапа таковы, что подавляющая часть телекоммуникационных технологий, аппаратных решений, программных средств и средств связи, которые мы вынуждены использовать в Российской Федерации, созданы за рубежом. Эти компьютерные, коммуникационные и связные решения поставляются нам в готовом виде, без права доступа к ним несертифицированных фирмами-производителями российских специалистов. Фирмы-производители при подготовке сертифицированных специалистов не проводят подготовки россиян по значительному кругу вопросов, среди которых обеспечение безопасности, удаленное управление и наладка. Для этих работ в России приглашаются иностранцы, которые производят замену оборудования и апгрейт программного обеспечения на новые версии без права доступа российских специалистов из эксплуатирующих организаций. Альтернативой этому зачастую является открытие международного канала полного доступа к оборудованию и удаленная отладка всех систем из-за рубежа фирмой-производителем. Документация к иностранному оборудованию и программному обеспечению всегда носит фрагментарный характер и содержит большие лакуны. При этом она предназначена только для эксплуатирующих организаций и не отвечает критериям доверия ни международным, ни российским стандартам безопасности.

Также надо учесть, что национальное законодательство США и стран их союзников содержит экспортные ограничения на производство упомянутых средств для связи и массовых коммуникаций без предоставления национальным спецслужбам предусмотренных разработчиками средств обхода протоколов безопасности и кодов вскрытия криптозащиты. Эти особенности (эксплойты) и присущие аппаратно-программным средствам уязвимости активно выясняются хакерскими группировками, эксплуатируются в корыстных целях как конкурентами в бизнесе, так и отдельными группами для совершения противоправных деяний. Именно слабости защитных механизмов и «заложенные» разработчиками уязвимости порождают в свою очередь в

хакерской среде целые «волны» создания вредоносных программ, «программ-шпионов» и средств перехвата управления компьютерами и средствами связи.

Также следует иметь ввиду спектр угроз безопасности, проистекающих из созданных искусственно социальных сетей, мессенджеров, международных облачных технологий, основанных на общедоступных и «слабых» Web-технологиях. Двойственный характер этих средств коммуникаций, с одной стороны, позволяет зарабатывать на рекламе таких сервисов, а с другой стороны, позволяет разыскивать и опосредованно детально изучать интересы и пристрастия людей, характер и направленность личности, слабые и сильные стороны пользователей таких сервисов. Эти технологии активно используются для пропаганды идеологии экстремизма и терроризма.

Однако в последние годы руководство России взяло курс на импортозамещение в сферах использования средств связи и массовых коммуникаций, наиболее чувствительных для обороны и безопасности страны. При этом, особенно после введения против отдельных госструктур международных санкций, происходит бурный рост отечественных научно-технических разработок средств безопасности, элементной базы и программного обеспечения. Укрепляется законодательная и ведомственная нормативно-правовая база обеспечения защиты интересов государства, личности и общества в информационной сфере.

Целью настоящего учебно-методического пособия по дисциплине «Техническое противодействие компьютерной разведке» являются теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий выявления и противодействия формам, методам и приемам проведения компьютерной разведки. В нем рассматриваются цели, роли и способы проведения современной компьютерной разведки, а также основания, формы, методы и приемы технического противодействия в условиях иностранного технического доминирования в телекоммуникационных технологиях и сетях связи. В пособии также исследуются международные и российские стандарты и нормативные требования в сфере управления информационной безопасностью, что способствует выработке у студентов знаний и навыков

организации технического противодействия методам и средствам проведения компьютерной разведки, применяемой против российских объектов информатизации.

Структура пособия:

В первой главе рассматриваются цели и задачи компьютерной разведки, формы и условия проведения компьютерной конкурентной разведки, использования методов компьютерной разведки в меркантильных противоправных целях, а также в противоправных политических целях для реализации идеологии терроризма и экстремизма. Также в ней рассматриваются роль, место и формы организационно-юридического и технического противодействия методам компьютерной разведки, осуществляемого на объектах российской информационной инфраструктуры.

Во второй главе дается обзор методов выявления признаков и фактов проведения компьютерной разведки в широкополосных сетях, сетях общего доступа, современных беспроводных сетях связи, использование для этого на критически важных объектах информационной инфраструктуры штатных, общедоступных иностранных и специальных российских технологий мониторинга (как части «аудита» и в качестве самостоятельных инструментов). Также обозначаются правила оформления и проведения в России проверок на возможное наличие закладных аппаратных или программных средств компьютерной разведки.

Третья глава пособия посвящена правилам и стандартам оценки уязвимости систем для компьютерной разведки. В ней рассматриваются современные методы выявления уязвимости объектов информатизации для средств проведения компьютерной разведки, порядок проведения оценки эффективности принимаемых защитных мер. Дополнительно приводятся примеры из истории инцидентов безопасности, дается обзор их протекания и устранения последствий таких инцидентов.

Глава четвертая посвящена обзору средств и методов обнаружения вторжений в информационные системы. Здесь рассматриваются методы выявления и отражения компьютерных атак, проблемы и приемы «антихакинга» как части мер по выявлению признаков злонамеренного изучения открытых

сервисов и защитных механизмов системы. Отдельное внимание уделено современным системам обнаружения вторжений и атак.

Глава пятая посвящена системам противодействия программным закладкам, где рассматриваются формы и методы противодействия программным закладкам, антивирусные средства, дается необходимое понятие о системах-ловушек.

Шестая глава пособия полностью посвящена комплексу мер технического противодействия компьютерной разведке. В нее входит разработка вариантов совершенствования имеющихся мер технического противодействия компьютерной разведке на российских объектах информатизации. Также дается обзор современных и перспективных российских аппаратных, программных и аппаратно-программных комплексов технического противодействия компьютерной разведке, описываются их назначение и функциональные возможности.

1. Цели и задачи компьютерной разведки, формы и условия ее проведения. Роль, место и формы противодействия компьютерной разведке

Современная компьютерная разведка (далее - КР) не является в настоящее время (и на дальнюю перспективу) самостоятельным видом деятельности каких-либо групп. Она используется лишь как наиболее безуликовый, высокоэффективный, но все-таки инструмент для реализации тех или иных планов каких-либо групп, организаций и объединений в интересах достижения политических, экономических или преступных целей (общуголовных, экстремистских или террористических). КР не локализуется только внутри государств, а в наиболее опасных ее проявлениях активно принимает межгосударственный характер телекоммуникационных систем и сетей связи, а также разделение юрисдикций национальных спецслужб и силовых структур. КР использует в качестве среды общедоступные системы телекоммуникаций и сети связи, стандартные сервисы и протоколы общего пользования. Подавляющая часть технических решений этих систем и сетей не только создана за рубежом, но и носит глобальный характер.

1.1. Цели, задачи и особенности проведения компьютерной конкурентной разведки, использования методов компьютерной разведки в меркантильных противоправных целях, а также в противоправных политических целях для реализации идеологии терроризма и экстремизма

Настоящий этап развития массовых телекоммуникаций характерен глобальной связью национальных компьютерных сетей широкополосного доступа к сетевым ресурсам, которые в силу этой доступности и отсутствия границ в глобальных сетях становятся международными. Для современного этапа характерными являются массовые факты применения государственными, коммерческими компаниями и корпорациями, а также экстремистскими, террористическими и криминальными структурами информационных операций и информационных атак (далее - ИОА). КР используется лишь как наиболее безуликовый, высокоэффективный, но все-таки инструмент для реализации ИОА в интересах достижения политических, экономических или преступных целей (общеуголовных, включая хакерские, экстремистских или террористических). Ежегодно в мире (и в России) растет число преступлений корыстной направленности, совершаемых с использованием информационно-телекоммуникационных технологий, которые почти невозможно совершить (кроме физического хищения носителей или физического уничтожения информации вместе со средствами ее автоматизированной обработки) без предварительного применения средств и методов КР. Значительный ряд преступлений в сфере информационно-телекоммуникационных технологий просто невозможен без противоправного применения средств и методов КР.

Таким образом, более полное толкование термина КР можно сформулировать следующим образом. Компьютерная разведка - это деятельность, направленная на получение информации из информационных систем, подключенных напрямую или через средства связи к компьютерным сетям открытого типа, включая информацию из соцсетей, сайтов, порталов и сетевых средств коммуникаций (чатов и видеочатов, месенджеров, форумов, IP-телефонии и др.), информации об особенностях построения и

функционирования защищенных и открытых информационных систем и сетей конкурентов, госструктур и других объектов проникновения.

Целью компьютерной разведки, как правило, является добывание сведений о предмете, конечных результатах, формах и способах деятельности субъектов, являющихся пользователями информационно-вычислительной сети, а также об используемом аппаратном и программном обеспечении, протоколах управления и информационного взаимодействия и используемых средствах и методах защиты информации.

Компьютерная разведка - новейший вид технической разведки. Ее появление связано с развитием в современной военной науке концепции информационной войны. Например, в США выпущены два полевых устава FM-100-5 и FM-100-6, излагающие основы информационной войны и информационной операции. Цель информационной войны - обеспечение своему государству информационного господства, которое в наш век - век информации - представляется необходимым условием того, чтобы военно-экономический потенциал государства смог привести к реальной победе. Важнейшая роль в достижении информационного господства отводится компьютерной разведке, ведущейся в информационных потоках, которые в гигантских количествах производятся всеми государственными и частными организациями, а также отдельными индивидуумами. Она включает в себя три основных направления:

- разведку в информационно-вычислительных компьютерных сетях (включая соцсети, Web-сервисы удаленных компьютерных ресурсов), потоках связи для доступа к содержанию передаваемой информации и сообщений;

- разведку в бумажных и электронных средствах массовой информации;

- разведку в неперiodических изданиях, в том числе в открытых и так называемых «серых» (т.е. не имеющих грифа секретности, но не предназначенных для массового распространения - отчетах о НИР, аналитических справках, деловой переписке, диссертациях и т.п.).

Компьютерная разведка представляет собой комплекс взаимосвязанных действий оперативного и технического

характера. Иногда встречается важный для понимания глубины процессов термин «Социо-технические системы» (далее - СТС), которые используются и как объект проникновения КР, и как среда, в которой производится КР.

Компьютерную разведку разделяют на добывающую и обрабатывающую. В полевом уставе США «FM 100-6» приводится иерархия ситуационной осведомленности (рис. 1.1.), представляющая собой пирамиду, в основании которой лежат данные.



Рис. 1.1. Иерархия ситуационной осведомленности как цели КР.

На втором уровне находится информация, получаемая путем обработки разведданных. Изучение информации приводит к формированию знаний (следующий уровень осведомленности), а знания посредством суждения способствуют пониманию (верхний уровень). Ситуационные знание и понимание ситуации являются одной из целей КР.

Задача добывающей разведки состоит в получении данных, а обрабатывающей - в преобразовании данных в информацию и приведение ее в форму, удобную для пользователя.

Добывающая разведка подразделяется на предварительную и непосредственную.

Задача предварительной разведки - получение сведений о самой автоматизированной системе обработки данных (далее-АСОД), составе информационной системы объекта проникновения и особенностях ее защитных механизмов. Промежуточная цель этих действий предварительной разведки -

подобрать данные, необходимые для последующего незаметного проникновения в целевую АСОД или блокирования ее работы. Цели предварительной разведки достигаются путем добывания открытых и закрытых сведений. К открытым сведениям можно отнести данные о характере и режиме работы АСОД объекта разведки; квалификации его персонала; составе и структуре самой АСОД, используемом программном обеспечении; протоколах управления и взаимодействия; средствах и методах защиты информации, используемых в АСОД. Для получения этих сведений нет необходимости прибегать к приемам оперативной работы (подкупу персонала, краже документации и т.п.). Эти сведения, как правило, не являются закрытыми и могут быть получены при перехвате сетевого трафика интересующей АСОД либо при попытке установить сетевое соединение непосредственно с самой АСОД, когда по характеру получаемого отклика можно сделать соответствующие выводы.

Установление первичного контакта с АСОД противника, как правило, еще не дает доступа к интересующей информации или возможности захвата управления информационной системой. Для этого необходимо получить дополнительные сведения «закрытого» характера. К таким защищаемым «закрытым» сведениям относятся пароли, коды доступа, информация о принятых в АСОД правилах разграничения доступа, сетевые адреса вычислительных средств атакуемой системы. Для получения подобных сведений существуют разнообразные программные средства. К ним относятся, например, программы-снифферы - прослушивающие сети, считывающие первые 128 бит каждого файла, в которых нередко помещается служебная информация о самом файле и об АСОД, а также автоматически анализирующие состав информационного обмена и получающие данные для дальнейшей атаки. Существуют также специальные программы подбора паролей.

Помимо ключей, интерес представляет перехват кусков зашифрованного текста с заранее известным содержанием. Это позволяет выделить из шифрограммы секретный ключ, который используется для дальнейшего криптоанализа всего текста.

Успеху подобных программ способствуют многочисленные ошибки в современном программном обеспечении, что, как

выясняется, является следствием постоянного воздействия на разработчиков со стороны национальных спецслужб на основании национальных законов (Телекоммуникационный акт 1996 года, поправка Джейсона-Вейника и Патриотический акт 2001 года в США и др.), призванных обеспечить национальные интересы и безопасность государствам, где разрабатываются средства связи и массовых коммуникаций.

Сведения, собранные подобным образом об АСОД объекта атаки, открывают путь к добыванию информации, интересующей заказчика, т.е. к ведению непосредственной разведки либо к совершению информационной атаки, заключающейся в искажении данных или блокировании нормальной работы сетевых сервисов. Также особым, получившим широкое распространение методом КР является применение комплекса средств для незаметного владельцам перехвата управления ЭВМ. Имеются в хакерской среде стандартные средства и оригинальные разработки программ-демонов, невидимых для антивирусов и перехватывающих все команды управления ИС для дальнейшего негласного использования ее ресурсов в интересах атакующей стороны, иногда создавая управляемые из единого центра «робосети» (Бот-сети), которые могут незаметно для владельцев выполнять негласные согласованные действия. Известны случаи аренды Бот-сетей для противоправных действий.

На стадии непосредственной разведки, как и на всех остальных, добываются не только закрытые, но также открытые сведения. Важнейшим достоинством перехвата открытых сведений при ведении компьютерной разведки является то, что эти сведения могут быть получены без нарушения принятых в АСОД правил разграничения доступа к информации.

Сбором и анализом открытых сведений в сетях сейчас официально занимается множество организаций, которые за определенную плату выполняют заказы на поиск той или иной информации. Любой пользователь сети Интернет также может самостоятельно вести поиск и анализ требуемой информации с помощью известных поисковых машин популярных Web-сервисов.

Добывание закрытых сведений всегда связано с несанкционированным доступом к информации противника и

имеет своим следствием утечку защищаемой информации. Получение закрытых сведений осуществляется как в самой АСОД объекта, так и в информационно-вычислительных сетях, внешних по отношению к АСОД. Во внешних сетях перехватываются те сообщения, которые объект разведки пересылает внешним адресатам, либо, в случае виртуальной сети, те сообщения, которые циркулируют между отдельными сегментами АСОД.

Можно выделить следующие способы перехвата закрытых сведений во внешних сетях:

- изменение маршрутизации при пересылке сообщений, что позволяет отправлять информацию через «свой» сервер, на котором производится перехват и запись данных;
- чтение электронной почты, которая, как правило, является легкой добычей и на сервере отправителя, и на сервере получателя;
- фальсификация сервера (сайта) адресата, что в случае успеха позволяет выманить у отправителя ту или иную закрытую информацию.

Программное проникновение в АСОД объекта с целью ведения разведки может осуществляться несколькими способами. Отдельную группу таких способов составляет проникновение через несетевые периферийные устройства (клавиатуру, дисководы и т.п.). Набор методов проникновения достаточно широк и определяется квалификацией взломщика и степенью несовершенства установленных на объекте систем защиты от несанкционированного доступа.

Считается, что абсолютно надежных систем защиты на сегодняшний день не существует. Например, известны приемы нарушения нормальной работы криптографических микросхем в системах разграничения доступа, начиная от нагревания и облучения и кончая применением моделей стимуляции направленных ошибок, которые позволяют получить секретные ключи, хранящиеся в памяти этих микросхем. Принципиальное отличие проникновения через несетевые периферийные устройства от остальных методов заключается в том, что для его выполнения необходимо физическое присутствие злоумышленника на объекте вычислительной техники. Это позволяет защищающейся стороне применить хорошо

отлаженный механизм организационно-технических мер защиты. Вокруг объекта создается контролируемая территория, на которой не допускается присутствие посторонних людей; к работам в АСОД допускается ограниченный круг лиц; ведется тщательный учет и анализ всех производимых в АСОД работ; учитываются используемые носители информации и т.п.

Наиболее многочисленная и динамично развивающаяся группа способов программного проникновения в АСОД противника - это проникновение из внешних сетей. Можно выделить два основных пути такого проникновения: проникновение с использованием паролей и идентификаторов, найденных в результате предварительной разведки, а также поиск ошибок (т.н. «люков», «черных ходов», «лазеек») в программном обеспечении, используемом в АСОД. Большое количество «люков», «эксплойтов» объясняется ошибками авторов и требуемой для национальных спецслужб «предусмотрительностью» авторов программного обеспечения. После разоблачений «Викиликс» и Э.Сноудена стало во всем мире очевидно, что «люки» оставляются автором программного обеспечения преднамеренно, чтобы создать национальным спецслужбам возможности по удаленному доступу и управлению информационными системами в обход подсистем безопасности, а многочисленные хакеры находят эти «люки» и используют их в своих целях, в том числе для добывания сведений из системы пользователя. То есть, широкую огласку получили данные о проведении АБН и другими разведведомствами стран НАТО крупномасштабных глобальных негласных разведывательных проектов с использованием программного обеспечения с незадекларированными возможностями. В редких случаях авторы программно-аппаратных решений устанавливают «люки» для облегчения процесса отладки программы, а потом их ликвидируют.

Из-за указанных процессов ежегодно растет число выявляемых критических уязвимостей и «эксплойтов» в общедоступных аппаратно-программных решениях, активно эксплуатируемых хакерскими группами в противоправных целях.

Однако недостаточно лишь добраться до винчестера противника и «скачать» с него несколько гигабайт данных.

Необходимо восстановить удаленные файлы противника, тщательно разобраться в полученном объеме сведений. Эту функцию выполняет обрабатывающая разведка. Специальные программы позволяют определить тип фрагмента когда-то удаленного файла (текстовый, графический, исполняемый и т.п.) и восстановить содержащуюся в нем информацию; сопоставить и логически увязать имеющиеся файлы; устранить дублирование информации; отобрать по ключевым словам и ассоциированным понятиям только ту информацию, которая в данный момент необходима заказчику. Обработке подвергаются данные, полученные как в отдельном средстве вычислительной техники, так и в информационно-вычислительных сетях, при этом сеть представляет дополнительные возможности по обработке. Посредством анализа трафика можно контролировать гигантские потоки сведений, производить отбор, накопление и обработку не всех данных подряд, а только тех, которые представляют интерес для конечного потребителя. Для ведения экспресс-анализа в сети созданы специальные программы, так называемые ноу-боты – специальные программные продукты, незаметно перемещающиеся от компьютера к компьютеру с возможностью размножения, которые отслеживают состояние дел и передают сводную информацию по каналам обмена данными. С помощью средств компьютерной разведки можно не только анализировать данные, циркулирующие во всей сети, безотносительно к их источнику, но и отслеживать деятельность конкретных организаций и отдельных лиц, выявлять источника распространения какой-либо информации, что часто и является средством проведения информационной операции или атаки (ИОА).

В связи с высокой степенью угрозы безопасности информации, обрабатываемой в информационно-вычислительных сетях, все большее количество пользователей сети применяют для защиты своей информации шифрование. По этой причине одной из задач обрабатывающей компьютерной разведки является проведение элементов криптоанализа. Криптоанализ - наука о раскрытии алгоритмов шифрования, подборе ключей и восстановлении информации из зашифрованного сообщения. Поскольку в криптоанализе широко используются компьютерные

методы обработки информации, то отчасти его можно отнести к обрабатывающей технической разведке. Например, несложные шифры могут быть взломаны компьютером автоматически, без участия человека. К качественному скачку в криптоанализе приводят современные информационные технологии. Так, если подбор ключа на отдельном компьютере может занять много лет, то применение специальных программ с задействованием упомянутых Бот-сетей, негласно использующих свободные избыточные вычислительные ресурсы ЭВМ, позволяет задействовать параллельно десятки и сотни тысяч компьютеров для сокращения времени подбора ключа до считанных недель. В то же время криптоанализ может быть отнесен к компьютерной разведке лишь по методу применения компьютерных технологий для проникновения к целевой защищаемой информации. При взломе сколько-нибудь серьезных шифров решающую роль играет подготовка, интуиция и опыт криптоаналитика, знание особенностей использования так называемых методов «социальной инженерии» для закрытых от посторонних СТС.

Но нельзя забывать, что зарубежные операционные системы, надстройками к которым и являются прикладные программы атакуемых информационных систем, изначально делаются с недокументированными функциями удаленного доступа к управлению и защищаемым данным на уровне файловых систем, а криптозащита на уровне файловой системы сама использует зарубежные алгоритмы шифрзащиты, ключи доступа к которым переданы разработчиками в национальные спецслужбы. Но возможности доступа (например, «эксплойты») извне к предусмотренным разработчиками недокументированным функциям зарубежных информационных систем все чаще становятся достоянием хакеров, как было упомянуто ранее.

В связи с тем, что изучение вопросов защиты информации в средствах вычислительной техники началось сравнительно недавно, встречаются различные точки зрения на компьютерную разведку и ее место среди угроз безопасности информации.

Как известно, все угрозы безопасности информации можно разделить на 4 типа: уничтожение, изменение, хищение, блокирование.

Компьютерная разведка, как и любая другая разведка, занимается не только хищением информации. Активное воздействие на информацию не предполагается в случаях, когда в целях маскировки несанкционированного доступа модифицируется некоторая служебная, второстепенная с точки зрения добывания, информация в операционной системе и средствах защиты АСОД, являющейся целью проникновения. По этой причине к компьютерной разведке теперь относят все средства активного воздействия на информационные системы противника - почтовые и логические бомбы, электронные черви, SYN-наводнения, атаки типа «салами», большинство вирусов и другие средства и методы из арсенала криминальных хакеров, используемые для дальнейших махинаций с банковскими счетами, кражи для перепродажи персональных данных и другую ликвидную на черном хакерском рынке информацию. Также уже считаются компьютерной разведкой и способы несанкционированного копирования лицензионных программных продуктов и взламывания их защиты, если целью этих действий является получение защищаемой информации, в том числе и в интересах нарушения авторского права на коммерческие и научные полезные модели и изобретения, а также для дальнейшего незаконного доступа к услугам.

В экстремистских и террористических целях компьютерную разведку используют для поиска на форумах, в чатах и соцсетях лиц, в чьих типичных реакциях на те или иные материалы и обсуждение каких-либо «чувствительных вопросов» содержатся признаки возможного сочувствия идеологии терроризма и экстремизма. С такими лицами завязывается контакт, продолжается отслеживаться их состояние. Затем выявленные и взятые в изучение люди склоняются либо к выезду в места проведения боевых действий на ближнем востоке, либо на обучение в центры подготовки боевиков. До первых уголовных дел по участию, или пособничеству террористической деятельности, также отмечались десятки фактов склонения к выезду в лагеря подготовки боевиков молодых мусульманских женщин-вдов с детьми. Также методы компьютерной разведки применялись для розыска через сеть Интернет установочных данных участников

контртеррористических операций и их родственников. Также отмечались случаи применения приемов КР для выяснения и использования в дальнейшем «тонкостей» функционирования интернет-технологий (сервисов, в том числе и криптозащищенных сервисов общения через соцсети) для управления якобы стихийными протестными акциями с экстремистскими призывами. Также используются методы КР, характерные для запутывания следов после компьютерных атак, зеркальные анонимные серверы, применяемые для пропаганды идей терроризма и экстремизма, заказные распределенные компьютерные атаки через Бот-сети на официальные сетевые ресурсы органов гос. власти и ведомств, участвующих в противодействии терроризму и экстремизму. Имеются сведения о разовых и на постоянной основе фактов использования хакерских групп для отмыwania денежных средств по финансированию террористических и экстремистских организаций, прикрытия их операций по конспиративной связи между их участниками.

1.2. Роль, место и формы организационно-юридического и технического противодействия методам компьютерной разведки объектов российской информационной инфраструктуры

Сложившаяся государственная система информационной безопасности по своей структуре во многом повторяет геополитическую конструкцию российского государства (рис. 1.2). В ней просматривается «вертикаль» от Президента — председателя Совета безопасности РФ — до субъектов хозяйствования, физических и юридических лиц, сталкивающихся в регионах с проблемами данного профиля.

Силловые ведомства, представленные в Совете безопасности РФ своими руководителями, активно работают на уровне межведомственных комиссий (по защите гостайны и др.). Их территориальные органы соответственно представлены своими руководителями в комиссиях по ИБ на уровнях федерального округа и региона. При этом, естественно, в системе (см. рис. 1.2)

участвуют и органы представительной власти (законодательных собраний федерального и регионального уровней).

Одним из важнейших слоев, обеспечивающих успех функционирования системы (см. рис. 1.2), представляет собой региональный срез проблемы, который наиболее емко характеризует механизм, изображенный на рис. 1.3. Суть его сводится к управлению региональным информационным пространством в контексте обеспечения его безопасности. На рис. 1.3 представлены все основные субъекты (комиссия по ИБ, экспертные советы, органы исполнительной и представительной ветвей власти, база знаний и данных ИОА, территориальные органы и предприятия, программа и обеспечение ИБ) и процедуры (выработка критериев, модернизация и перестройка, анализ последствий ИОА) обеспечения региональной ИБ. Ключевым звеном структуры является условный оператор оценки величины риска в сравнении с фоном, чему предшествует риск-анализ объектов информатизации региона. Координатором данного механизма является региональная комиссия по ИБ, создаваемая при губернаторе (главе администрации) субъекта РФ.

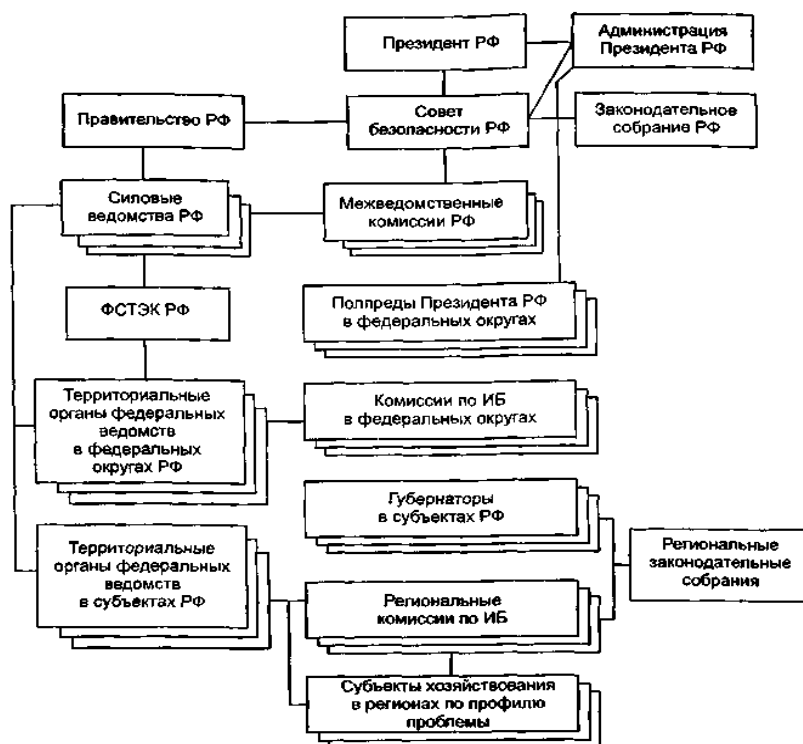


Рис. 1.2. Государственная система информационной безопасности РФ.

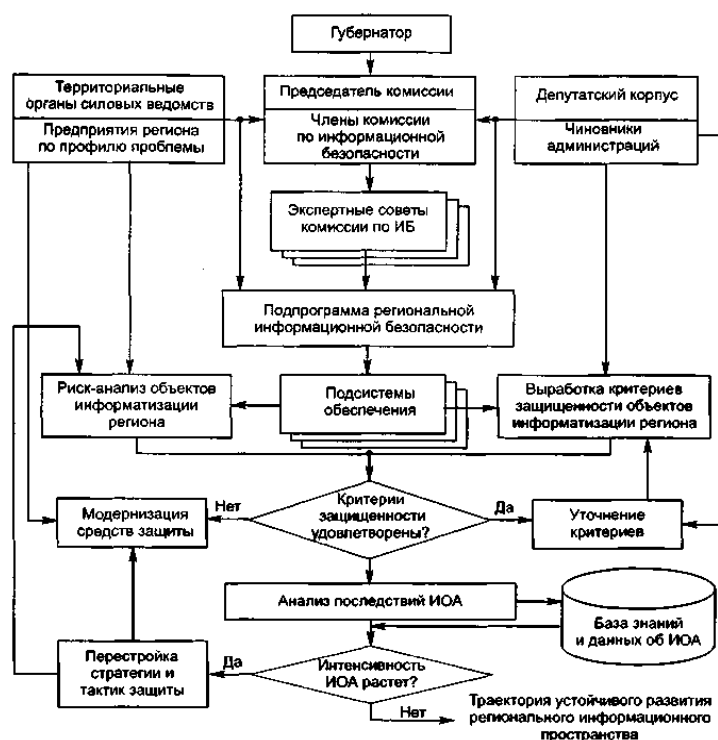


Рис. 1.3. Структурная схема управления безопасностью регионального информационного пространства

Рисковый режим законотворчества в области информационной безопасности (ИБ) базируется на результатах мониторинга правонарушений в информационной сфере (ПНИС), совершаемых в информационном пространстве. Механизм подобного управления представлен на рис. 1.4. Суть его сводится к текущему риск-анализу ПНИС. В частности, для региона региональная комиссия по ИБ совместно с территориальными органами федеральных ведомств определяет допустимые пороги (допуски) риска ПНИС. Периодически (в определенные периоды оценки) осуществляется сравнение текущих значений риска с установленными порогом (здесь может быть взята за основу федеральная и общемировая статистика). Выход за границы допусков порождает необходимость модернизации организационно-правовой основы (региональной и/или федеральной), которая по соответствующим инициативам в установленном порядке может быть реализована компетентными органами законодательной и исполнительной власти соответствующего уровня.

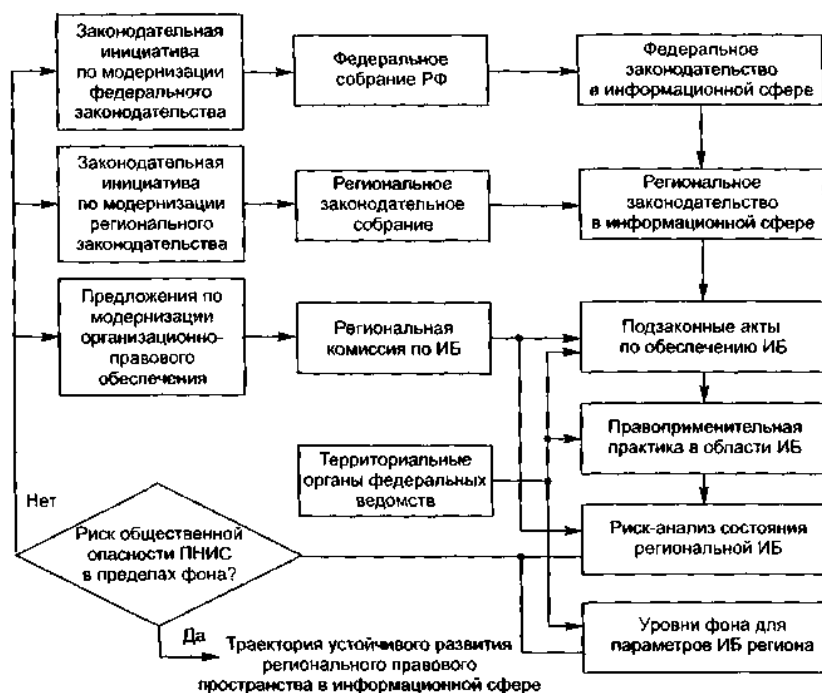


Рис. 1.4. Механизм законотворчества в области информационной безопасности

Механизм собственно риск-анализа поясняет рис. 1.5, где предлагается находить риск по отдельным видам ПНИС, исходя из их частоты, ущерба и латентности.

Организационный механизм противодействия угрозам информационной безопасности должен включать (рис. 1.6) структуры стратегического и тактического управления, информационно-аналитическую структуру. Они должны быть снабжены соответствующим ресурсным и методическим обеспечением. На острие противодействия находится объект назначения информационного оружия (предприятие и/или организация региона), снабженный средствами обнаружения и пресечения угроз информационной безопасности, а также средствами нейтрализации их последствий.

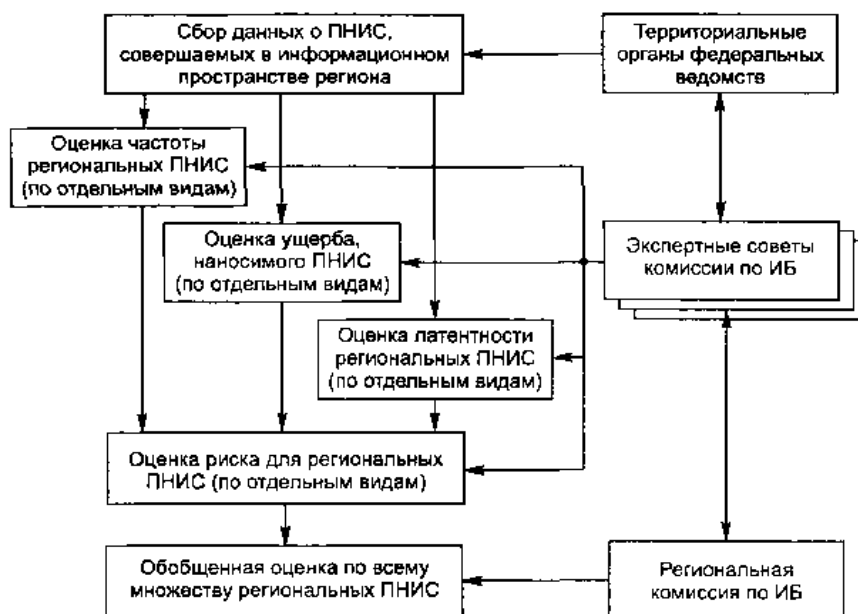


Рис. 1.5. Механизм риск-анализа региональной информационной безопасности



Рис. 1.6. Структурная схема управления противодействием ИОА на региональном уровне

Достаточно большое многообразие организационно-правовых задач может быть сведено к вышеуказанному минимаксному решению, где стержневым параметром является риск, оцененный в некоторых порогах (допусках). Вышеизложенный механизм носит достаточно универсальный характер и потому может быть с успехом адаптирован к реальной специфике конкретного региона любой цивилизованной страны, имеющей проблемы противодействия угрозам информационной безопасности и противодействия методам КР.

Однако следует добавить, что этот организационный механизм противодействия методам КР, кроме федеральных законов и постановлений Правительства России, реализуется в настоящее время в России шестью дополняющими друг друга группами документов государственных «регуляторов» данной сферы. С организационной стороны его дополняют документы Росстандарта в сфере информационной безопасности (этот набор будет рассмотрен ниже на следующих занятиях), директивными документами Минкомсвязи России, его подчиненной структуры - Роскомнадзора России (в части организации защиты персональных данных и контроля блокирования доступа к запрещенным Минюстом России информационным ресурсам) и его самостоятельного партнера ФГУП «Главный радиочастотный центр» России (в части разработки и контроля соблюдения частотно-территориальных планов субъектов Федерации). Сферу технической защиты информации для госсектора организуют и контролируют три межведомственных «регулятора» - ФСТЭК России (в части ТЗИ) подчиняется Минобороны России, ФСБ России (в части криптозащиты конфиденциальной и секретной информации, а также использования ГИС СОПКА на критических объектах информационной инфраструктуры страны, например, на объектах жизнеобеспечения, атомной и обычной энергетики, Минобороны, оборонной промышленности, транспорта, спецсвязи, силовых структур, представительств России за рубежом), подчиняющейся Президенту страны, а также в сфере правительственной и спецсвязи таким регулятором является ФСО России. ФСБ России, СВР России, ФСО России и Главное разведывательное управление Генерального штаба Минобороны России добывают информацию о возможностях иностранных

технических разведок, включая компьютерную разведку зарубежных государств и организаций, которую ФСТЭК России через уполномоченные и аккредитованные закрытые структуры изучает, проверяет, анализирует и обобщает в отдельные методические материалы, составляющие модель иностранной технической разведки (действует на определенный период, затем обновляется).

Далее эту модель, по запросам заинтересованных и уполномоченных организаций и ведомств, которым она нужна для непосредственного применения, ФСТЭК России высылает им вместе с методиками применения для самостоятельной разработки (или с привлечением уполномоченных и аккредитованных ФСБ и ФСТЭК структур) комплекса мер противодействия иностранной технической разведке, включая КР. Именно конкретные организации, информационные сети и системы которых могут быть объектами проникновения и компьютерных атак, и реализуют весь комплекс мер технического противодействия КР. Как применяются эти комплексы мер, эффективны ли они, периодически (периодичность определяется законодательством и Правительством России) проверяется «регуляторами» в своей сфере ответственности, указанной выше.

Для организаций негосударственных форм собственности, документы Росстандарта, ФСБ России, ФСТЭК России носят рекомендательный характер, кроме требований Роскомнадзора России, ФСБ России и ФСТЭК России в сфере защиты персональных данных, обязательных для организаций, предприятий и структур всех форм собственности. Эти, назовем их для краткости «коммерческие», организации, ориентируясь на требования безопасности государственных «регуляторов», на основе международных российских стандартов управления информационной безопасностью применяют общепринятые мировым бизнесом правила в условиях определенного и контролируемого риска. То есть, на свой собственный «страх и риск», самостоятельно оценивая соотношение между рисками и возможными потерями, если меры безопасности окажутся недостаточными.

Контрольные вопросы:

1. Чем вызваны и в чем заключаются задачи проведения компьютерной разведки?
2. Какие факторы и условия облегчают ее проведение?
3. Какие меры организационно-правового характера применяются в России для противодействия компьютерной разведке?
4. Какие меры инженерно-технического характера применяются в мире для противодействия компьютерной разведке?
5. Какие вы знаете российские особенности форм и методов, применяемых для технического противодействия компьютерной разведке?

Задания для самостоятельной работы к главе 1:

Вариант №1. Самостоятельно найти в открытых источниках примеры использования средств конкурентной компьютерной разведки, обосновать свой выбор.

Вариант №2. Самостоятельно найти в открытых источниках примеры использования методов компьютерной разведки для достижения политических целей, обосновать свой выбор.

Вариант №3. Самостоятельно найти в открытых источниках примеры использования методов компьютерной разведки для реализации идеологии терроризма или экстремизма, обосновать свой выбор.

Вариант №4. Самостоятельно найти в открытых источниках пример противодействия государства использованию методов компьютерной разведки на организационно-правовом уровне, оценить эффективность принятых мер безопасности.

Вариант №5. Самостоятельно найти в открытых источниках пример технического противодействия государства использованию методов компьютерной разведки во враждебных России целях, оценить эффективность принятых мер безопасности.

2. Методы выявления признаков и фактов проведения компьютерной разведки

Для выявления признаков и фактов проведения КР необходимо уяснить, какие формы и методы используются в КР.

2.1. Компьютерные атаки, основные понятия и определения, классификация атак, этапы реализации атак, основные механизмы реализации атак, реализация атак, завершение атаки

Основные определения и понятия

Атакой на информационную систему называются преднамеренные действия злоумышленника, использующие уязвимости информационной системы и приводящие к нарушению доступности, целостности и конфиденциальности обрабатываемой информации. Устранение уязвимости информационной системы приводит к устранению и самой возможности реализации атак. Существует три типа атак:

- «Разведка». Эти атаки включают ping sweeps, передачу DNS-зоны, разведку с помощью e-mail, сканирование TCP или UDP- портов и, возможно, анализ общественно доступных серверов с целью нахождения cgi-дыр.

- «Эксплойт» (exploit — использовать в своих интересах, злоупотреблять). Это компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака). Нарушители будут использовать преимущества скрытых возможностей или ошибок для получения несанкционированного доступа к системе.

- «Отказ в обслуживании» (Denial of Service, DoS). При такой атаке нарушитель пытается разрушить сервис (или компьютер), перегрузить сеть, перегрузить центральный процессор или переполнить диск.

Модели атак

Традиционная модель атаки строится по принципу «один к одному» или «один ко многим», т. е. атака исходит из одного источника. Разработчики сетевых средств защиты (межсетевых экранов, систем обнаружения атак и т. д.) ориентированы именно на традиционную модель атаки. В различных точках защищаемой

сети устанавливаются агенты (сенсоры) системы защиты, которые передают информацию на центральную консоль управления. Это облегчает масштабирование системы, обеспечивает простоту удаленного управления и т. д. Однако такая модель не справляется с распределенными атаками.

В модели распределенной атаки используются иные принципы. В отличие от традиционной модели в распределенной модели используются отношения «многие к одному» и «многие ко многим».

Распределенные атаки основаны на «классических» атаках типа «отказ в обслуживании», а точнее на их подмножестве, известном как Flood- или Storm-атаки (указанные термины можно перевести как «шторм», «наводнение» или «лавины»). Смысл данных атак заключается в посылке большого количества пакетов на атакуемый узел. Атакуемый узел может выйти из строя, поскольку он «захлебнется» в лавине посылаемых пакетов и не сможет обрабатывать запросы авторизованных пользователей. Однако в случае, если пропускная способность канала до атакуемого узла превышает пропускную способность атакующего или атакуемый узел некорректно сконфигурирован, к «успеху» такая атака не приведет. Но распределенная атака происходит уже не из одной точки Internet, а сразу из нескольких, что приводит к резкому возрастанию трафика и выведению атакуемого узла из строя.

Получили распространение следующие типы атак:

- удаленное проникновение (remote penetration). Атаки, которые позволяют реализовать удаленное управление компьютером через сеть. Например, NetBus или BackOrifice;
- локальное проникновение (local penetration). Атака, которая приводит к получению несанкционированного доступа к узлу, на котором она запущена. Например, Get Admin;
- удаленный отказ в обслуживании (remote denied of service). Атаки, которые позволяют нарушить функционирование или перегрузить компьютер через Internet. Например, Teardrop или trinOO;
- локальный отказ в обслуживании (local denial of service). Атаки, которые позволяют нарушить функционирование или перегрузить компьютер, на котором они реализуются. Примером

такой атаки является «враждебный» апплет, который загружает центральный процессор бесконечным циклом, что приводит к невозможности обработки запросов других приложений.

Классификация атак

Существуют различные типы классификации атак. Например, деление на пассивные и активные, внешние и внутренние, умышленные и неумышленные. Самым естественным и явным образом можно классифицировать существующие актуальные аномалии по типу источника или причины их возникновения. Пример такой классификации приведен на рис 2.1.

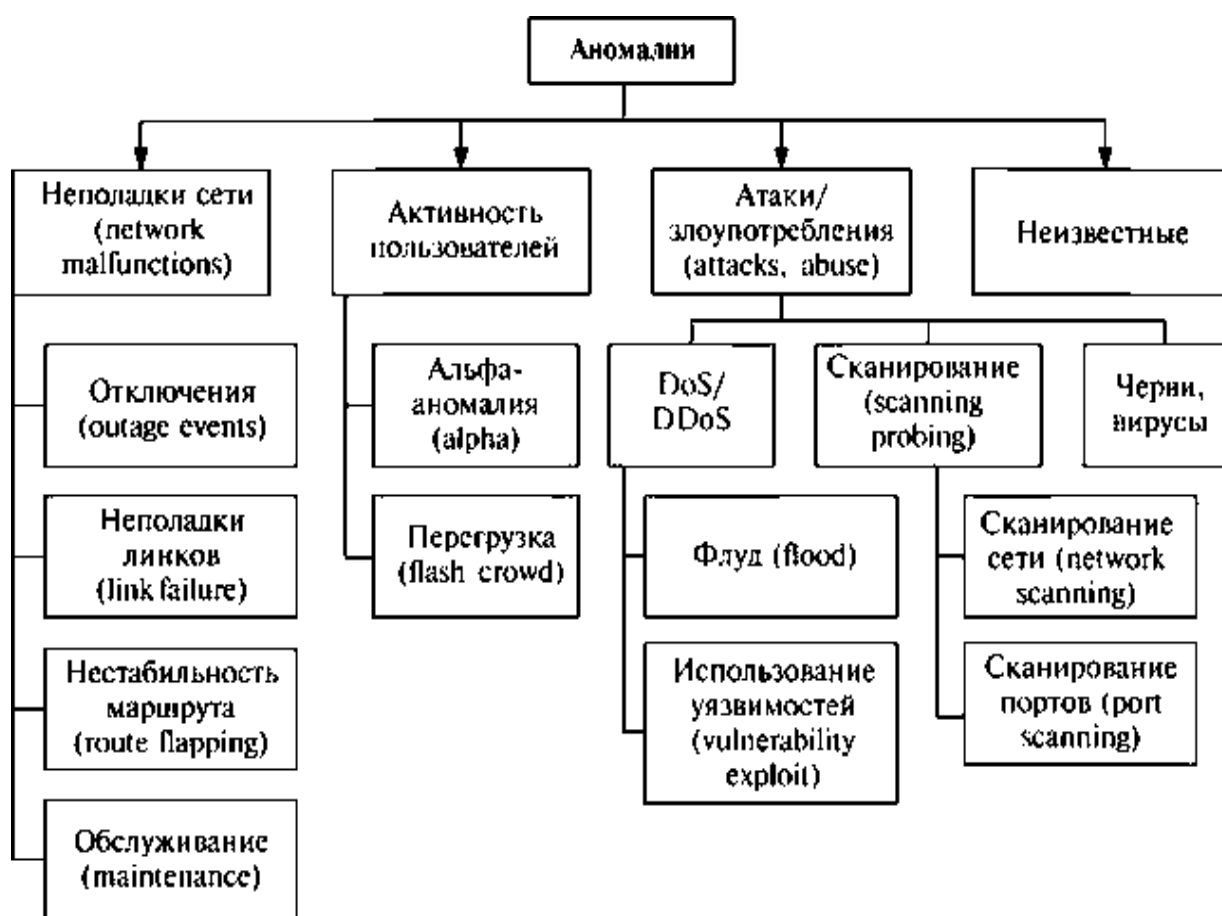


Рис. 2.1. Классификация аномалий в IP-сетях по типу

В табл. 1 представлены основные типы сетевых аномалий, их описание и основные характеристики. Приведенная систематизация данных об атаках и этапах их реализации дает необходимый базис для понимания технологий обнаружения атак.

Таблица 1. Основные типы аномалий в IP-сетях

Тип аномалии	Описание	Характеристики
Альфа-аномалия	Необычно высокий уровень трафика типа точка-точка	Выброс в представлении трафика байты/с, пакеты/с по одному доминирующему потоку источник — назначение. Небольшая продолжительность (до 10 минут)
DoS, DDoS атака	Распределенная атака типа отказ в обслуживании на одну жертву	Выброс в представлении трафика пакеты/с, потоки/с, от множества источников к одному адресу назначения
Перегрузка	Необычно высокий спрос на один сетевой ресурс или сервис	Скачок в трафике по потокам/с к одному доминирующему IP-адресу и доминирующему порту. Обычно кратковременная аномалия
Сканирование сети/портов	Сканирование сети по определенным открытым портам или сканирование одного хоста по всем портам с целью поиска уязвимостей	Скачок в трафике по потокам/с, с несколькими пакетами в потоках от одного доминирующего IP-адреса
Деятельность червей	Вредоносная программа, которая самостоятельно распространяется по сети и использует уязвимости операционных систем	Выброс в трафике без доминирующего адреса назначения, но всегда с одним или несколькими доминирующими портами назначения
Точка-мультиточка	Распространение контента от одного сервера многим пользователям	Выброс в пакетах, байтах от доминирующего источника к нескольким назначениям, все к одному (одним) хорошо известным портам
Отключения	Сетевые неполадки, которые вызывают падение в трафике между одной парой источник-назначение	Падение в трафике по пакетам, потокам и байтам обычно до нуля. Может быть долговременным и включать все потоки источник-назначение от или к одному маршрутизатору
Переключения потока	Необычное переключение потоков трафика с одного входящего маршрутизатора на другой	Падение в байтах или пакетах в одном потоке трафика и выброс в другом. Может затрагивать несколько потоков трафика

Этапы реализации атак

Можно выделить следующие этапы реализации атаки:

- предварительные действия перед атакой или «сбор информации»;
- собственно «реализация атаки»;
- завершение атаки.

Обычно, когда говорят об атаке, подразумевают именно второй этап, забывая о первом и последнем. Сбор информации и завершение атаки («заметание следов») в свою очередь также могут являться атакой и могут быть разделены на три этапа.

Сбор информации

Сбор информации — основной этап реализации атаки. Именно на данном этапе эффективность работы злоумышленника является залогом «успешности» атаки. Сначала выбирается цель атаки и собирается информация о ней:

- тип и версия операционной системы;
- открытые порты и запущенные сетевые сервисы;
- установленное системное и прикладное программное обеспечение и его конфигурация и т. д.

Затем идентифицируются наиболее уязвимые места атакуемой системы, воздействие на которые приводит к нужному злоумышленнику результату. Злоумышленник пытается выявить все каналы взаимодействия цели атаки с другими узлами. Это позволит не только выбрать тип реализуемой атаки, но и источник ее реализации. Например, атакуемый узел взаимодействует с двумя серверами под управлением ОС Unix и Windows NT. С одним сервером атакуемый узел имеет доверенные отношения, а с другим — нет. От того, через какой сервер злоумышленник будет реализовывать нападение, зависит, какая атака будет задействована, какое средство реализации будет выбрано и т. д. Затем, в зависимости от полученной информации и желаемого результата, выбирается атака, дающая наибольший эффект. Например, атака SYN-Flood. Сеансовый уровень отвечает за процедуру установления начала сеанса и подтверждение (квитирование) прихода каждого пакета от отправителя получателю. В Интернете протоколом сеансового уровня является протокол TCP (он занимает 4 и 5 уровни модели OSI). В отношении сеансового уровня очень широко распространена

специфичная атака класса «отказ в сервисе», основанная на свойствах процедуры установления соединения в протоколе TCP. Она получила название SYN-Flood (flood — большой поток).

При попытке клиента подключиться к серверу, работающему по протоколу TCP (а его используют более 80 % информационных служб, в том числе HTTP, FTP, SMTP, POP3), он посылает серверу пакет без информации, но с битом SYN, установленным в 1 в служебной области пакета — запросом на соединение. По получении такого пакета сервер обязан выслать клиенту подтверждение приема запроса, после чего с третьего пакета начинается собственно диалог между клиентом и сервером. Одновременно сервер может поддерживать в зависимости от типа сервиса от 20 до нескольких тысяч клиентов.

При атаке типа SYN-Flood злоумышленник начинает на своей ЭВМ создавать пакеты, представляющие собой запросы на соединение (т. е. SYN-пакеты) от имени произвольных IP-адресов (возможно даже несуществующих) на имя атакуемого сервера по порту сервиса, который он хочет приостановить. Все пакеты будут доставляться получателю, поскольку при доставке анализируется только адрес назначения. Сервер, начиная соединение по каждому из этих запросов, резервирует под него место в своем буфере, отправляет пакет-подтверждение и начинает ожидать третьего пакета клиента в течение некоторого промежутка времени (1...5 секунд). Пакет-подтверждение уйдет по адресу, указанному в качестве ложного отправителя в произвольную точку Интернета, и либо не найдет адресата вообще, либо чрезмерно «удивит» операционную систему на этом IP-адресе (поскольку она никаких запросов на данный сервер не посылала) и будет просто проигнорирован. А вот сервер при достаточно небольшом потоке таких запросов будет постоянно держать свой буфер заполненным ненужными ожиданиями соединений, и даже SYN-запросы от настоящих легальных пользователей не будут помещаться в буфер; сеансовый уровень просто не знает и не может узнать, какие из запросов фальшивые, а какие настоящие и могли бы иметь больший приоритет.

Традиционные средства защиты, такие как межсетевые экраны или механизмы фильтрации в маршрутизаторах, вступают в действие лишь на втором этапе реализации атаки, совершенно

«забывая» о первом и третьем. Это приводит к тому, что зачастую совершаемую атаку очень трудно остановить даже при наличии мощных и дорогих средств защиты. Пример тому — распределенные атаки. Логично было бы, чтобы средства защиты начинали работать еще на первом этапе, т. е. предотвращали бы возможность сбора информации об атакуемой системе. Это позволило бы если и не полностью предотвратить атаку, то хотя бы существенно усложнить работу злоумышленника. Традиционные средства также не позволяют обнаружить уже совершенные атаки и оценить ущерб после их реализации, т. е. не работают на третьем этапе реализации атаки. Следовательно, невозможно определить меры по предотвращению таких атак впредь.

В зависимости от желаемого результата нарушитель концентрируется на том или ином этапе реализации атаки. Например, для отказа в обслуживании подробно анализируется атакуемая сеть, в ней выискиваются лазейки и слабые места; для хищения информации основное внимание уделяется незаметному проникновению на атакуемые узлы при помощи обнаруженных ранее уязвимостей.

Основные механизмы реализации атак

Первый этап реализации атак — это сбор информации об атакуемой системе или узле. Он включает такие действия как определение сетевой топологии, типа и версии операционной системы атакуемого узла, а также доступных сетевых и иных сервисов и т. п. Эти действия реализуются различными методами.

Изучение окружения. На этом этапе нападающий исследует сетевое окружение вокруг предполагаемой цели атаки. К таким областям, например, относятся узлы Internet-провайдера «жертвы» или узлы удаленного офиса атакуемой компании. На этом этапе злоумышленник может попытаться определить адреса «доверенных» систем (например, сеть партнера) и узлов, которые напрямую соединены с целью атаки (например, маршрутизатор ISP) и т. д. Такие действия достаточно трудно обнаружить, поскольку они выполняются в течение достаточно длительного периода времени и снаружи области, контролируемой средствами защиты (межсетевыми экранами, системами обнаружения атак и т. п.).

Идентификация топологии сети. Существует два основных метода определения топологии сети, используемых злоумышленниками:

- изменение TTL (TTL modulation);
- запись маршрута (record route).

По первому методу работают программы traceroute для Unix и tracert для Windows. Они используют поле Time to Live («время жизни») в заголовке IP-пакета, которое изменяется в зависимости от числа пройденных сетевым пакетом маршрутизаторов. Для записи маршрута ICMP-пакета может быть использована утилита ping. Зачастую сетевую топологию можно выяснить при помощи протокола SNMP, установленного на многих сетевых устройствах, защита которых неверно сконфигурирована. При помощи протокола RIP можно попытаться получить информацию о таблице маршрутизации в сети и т. д.

Многие из этих методов используются современными системами управления (например, HP OpenView, Cabletron SPECTRUM, MS Visio и т.д.) для построения карт сети. И эти же методы могут быть с успехом применены злоумышленниками для построения карты атакуемой сети.

Идентификация узлов. Идентификация узла, как правило, осуществляется путем отправки при помощи утилиты ping команды ECHO-REQUEST протокола ICMP. Ответное сообщение ECHO-REPLY говорит о том, что узел доступен. Существуют свободно распространяемые программы, которые автоматизируют и ускоряют процесс параллельной идентификации большого числа узлов, например, fping или шпар. Опасность данного метода в том, что стандартными средствами узла запросы ECHO-REQUEST не фиксируются. Для этого необходимо применять средства анализа трафика, межсетевые экраны или системы обнаружения атак.

Это самый простой метод идентификации узлов. Однако он имеет два недостатка.

1. Многие сетевые устройства и программы блокируют ICMP- пакеты и не пропускают их во внутреннюю сеть (или, наоборот, не пропускают их наружу). Например, MS Proxy Server 2.0 не разрешает прохождение пакетов по протоколу ICMP. В результате возникает неполная картина. С другой стороны, блокировка ICMP-пакета говорит злоумышленнику о наличии

«первой линии обороны» — маршрутизаторов, межсетевых экранов и т. д.

2. Использование ICMP-запросов позволяет с легкостью обнаружить их источник, что, разумеется, не может входить в задачу злоумышленника.

Существует еще один метод идентификации узлов — использование «смешанного» режима сетевой карты, который позволяет определить различные узлы в сегменте сети. Но он не применим в тех случаях, в которых трафик сегмента сети недоступен нападающему со своего узла, т. е. этот метод применим только в локальных сетях. Другим способом идентификации узлов сети является так называемая разведка DNS, которая позволяет идентифицировать узлы корпоративной сети при помощи обращения к серверу службы имен.

Идентификация сервисов или сканирование портов. Идентификация сервисов, как правило, осуществляется путем обнаружения открытых портов (port scanning). Такие порты очень часто связаны с сервисами, основанными на протоколах TCP или UDP. Например, открытый 80-й порт подразумевает наличие Web-сервера, 25-й порт — почтового SMTP-сервера, 31337-й — серверной части троянского коня BackOrifice, 12345-й или 12346-й — серверной части троянского коня Net Bus и т.д.

Для идентификации сервисов и сканирования портов могут использоваться различные программы, в том числе и свободно распространяемые, например, nmap или netcat.

Идентификация операционной системы. Основной механизм удаленного определения ОС — анализ ответов на запросы, учитывающие различные реализации TCP/IP-стека в различных операционных системах. В каждой ОС по-своему реализован стек протоколов TCP/IP, что позволяет при помощи специальных запросов и ответов на них определить, какая ОС установлена на удаленном узле.

Другой, менее эффективный и крайне ограниченный, способ идентификации ОС узлов — анализ сетевых сервисов, обнаруженных на предыдущем этапе. Например, открытый 139-й порт позволяет сделать вывод, что удаленный узел, вероятнее всего, работает под управлением ОС семейства Windows. Для

определения ОС могут быть использованы различные программы, например, nmap или queso.

Определение роли узла. Предпоследним шагом на этапе сбора информации об атакуемом узле является определение его роли, например, выполнении функций межсетевого экрана или Web- сервера. Выполняется этот шаг на основе уже собранной информации об активных сервисах, именах узлов, топологии сети и т. п. Например, открытый 80-й порт может указывать на наличие Web- сервера, блокировка ICMP-пакета указывает на потенциальное наличие межсетевого экрана, а DNS-имя узла proхu.domain.ru или fw.domain.ru говорит само за себя.

Определение уязвимостей узла. Последний шаг — поиск уязвимостей. На этом шаге злоумышленник при помощи различных автоматизированных средств или вручную определяет уязвимости, которые могут быть использованы для реализации атаки.

Реализация атак

С этого момента начинается попытка доступа к атакуемому узлу. При этом доступ может быть как непосредственный, т. е. проникновение на узел, так и опосредованный, например, при реализации атаки типа «отказ в обслуживании». Реализация атак в случае непосредственного доступа также может быть разделена на два этапа:

- проникновение;
- установление контроля.

Проникновение. Проникновение подразумевает под собой преодоление средств защиты периметра (например, межсетевого экрана). Реализовываться это может быть различными путями. Например, использование уязвимости сервиса компьютера, «смотрящего» наружу, или путем передачи враждебного содержания по электронной почте (макровирусы) или через апплеты Java. Такое содержание может использовать так называемые «туннели» в межсетевом экране (не путать с туннелями VPN), через которые затем и проникает злоумышленник. К этому же этапу можно отнести подбор пароля администратора или иного пользователя при помощи специализированной утилиты, например, LOphtCrack или Crack.

Установление контроля. После проникновения злоумышленник устанавливает контроль над атакуемым узлом. Это может быть осуществлено путем внедрения программы типа «троянский конь» (например, NetBus или BackOrifice). После установки контроля над нужным узлом и «заметания» следов злоумышленник может осуществлять все необходимые несанкционированные действия дистанционно без ведома владельца атакованного компьютера. При этом установление контроля над узлом корпоративной сети должно сохраняться и после перезагрузки операционной системы. Это может быть реализовано путем замены одного из загрузочных файлов или вставки ссылки на враждебный код в файлы автозагрузки или системный реестр. Известен случай, когда злоумышленник смог перепрограммировать EEPROM сетевой карты и даже после переустановки ОС он смог повторно реализовать несанкционированные действия. Более простой модификацией этого примера является внедрение необходимого кода или фрагмента в сценарий сетевой загрузки (например, для ОС Novell Netware).

Цели реализации атак. Необходимо отметить, что злоумышленник на втором этапе может преследовать две цели. Во-первых, получение несанкционированного доступа к самому узлу и содержащейся на нем информации. Во-вторых, получение несанкционированного доступа к узлу для осуществления дальнейших атак на другие узлы. Первая цель, как правило, осуществляется только после реализации второй. То есть сначала злоумышленник создает себе базу для дальнейших атак и только после этого проникает на другие узлы. Это необходимо для того, чтобы скрыть или существенно затруднить нахождение источника атаки.

Завершение атаки

Этапом завершения атаки является «заметание следов» со стороны злоумышленника. Обычно это реализуется путем удаления соответствующих записей из журналов регистрации узла и других действий, возвращающих атакованную систему в исходное, «предатакованное» состояние.

2.2. Выявление признаков и фактов проведения компьютерной разведки в широкополосных сетях, сетях общего доступа, современных беспроводных сетях связи, на отдельных критически важных объектах информационной инфраструктуры. Использование штатных общедоступных технологий мониторинга в качестве самостоятельных инструментов. Программы анализа и мониторинга сетевого трафика, обзор снифферов

Существуют два не исключаяющих друг друга подхода к выявлению сетевых атак: анализ сетевого трафика и анализ контента. В первом случае анализируются только заголовки сетевых пакетов, во втором — их содержимое.

Конечно, наиболее полный контроль информационных взаимодействий может быть обеспечен только анализом всего содержимого сетевых пакетов, включая их заголовки и области данных. Однако с практической точки зрения эта задача является трудновыполнимой из-за огромного объема данных, которые приходилось бы анализировать. Современные СОВ начинают испытывать серьезные проблемы уже в сетях с производительностью 100 Мбит/с. Поэтому в большинстве случаев целесообразно использовать для выявления атак методы анализа сетевого трафика, в некоторых случаях сочетая их с анализом контента.

Сигнатура сетевой атаки концептуально практически не отличается от сигнатуры вируса. Она представляет собой набор признаков, позволяющих отличить сетевую атаку от других видов сетевого трафика.

Программы анализа и мониторинга сетевого трафика

Мониторинг трафика жизненно важен для эффективного управления сетью. Он является источником информации о функционировании корпоративных приложений, которая учитывается при распределении средств, планировании вычислительных мощностей, определении и локализации отказов, решении вопросов безопасности.

В недалеком прошлом мониторинг трафика был относительно простой задачей. Как правило, компьютеры

объединялись в сеть на основе шинной топологии, т. е. имели разделяемую среду передачи. Это позволяло подсоединить к сети единственное устройство, с помощью которого можно было следить за всем трафиком. Однако требования к повышению пропускной способности сети и развитие технологий коммутации пакетов, вызвавшее падение цен на коммутаторы и маршрутизаторы, обусловили быстрый переход от разделяемой среды передачи к высоко сегментированным топологиям. Общий трафик уже нельзя увидеть из одной точки. Для получения полной картины требуется выполнять мониторинг каждого порта. Использование соединений типа «точка-точка» делает неудобным подключение приборов, да и понадобилось бы слишком большое их число для прослушивания всех портов, что превращается в чересчур дорогостоящую задачу. Вдобавок сами коммутаторы и маршрутизаторы имеют сложную архитектуру, и скорость обработки и передачи пакетов становится важным фактором, определяющим производительность сети.

Одной из актуальных научных задач в настоящее время является анализ (и дальнейшее прогнозирование) самоподобной структуры трафика в современных мультисервисных сетях. Для решения этой задачи необходим сбор и последующий анализ разнообразной статистики (скорость, объемы переданных данных и т. д.) в действующих сетях. Сбор такой статистики в том или ином виде возможен различными программными средствами. Однако существует набор дополнительных параметров и настроек, которые оказываются весьма важными при практическом использовании различных средств. Приведем обзор основных возможностей некоторых распространенных программ-анализаторов сетевого трафика.

Программы-анализаторы сетевого трафика

BMExtreme. Это новое название хорошо известной многим программы Bandwidth Monitor. Ранее программа распространялась бесплатно, теперь же она имеет три версии, и бесплатной является только базовая. В этой версии не предусмотрено никаких возможностей, кроме, собственно, мониторинга трафика, поэтому вряд ли можно считать ее конкурентом других программ. По умолчанию BMExtreme следит как за интернет-трафиком, так и за

трафиком в локальной сети, однако мониторинг в LAN при желании можно отключить.

BWMeter. Эта программа имеет не одно, а два окна слежения за трафиком: в одном отображается активность в Интернете, а в другом — в локальной сети. Программа имеет гибкие настройки для мониторинга трафика. С ее помощью можно определить, нужно ли следить за приемом и передачей данных в Интернет только с этого компьютера или со всех компьютеров, подключенных к локальной сети, установить диапазон IP-адресов, порты и протоколы, для которых будет или не будет производиться мониторинг. Кроме этого, можно отключить слежение за трафиком в определенные часы или дни. Для каждого ПК можно задать максимальную скорость приема и передачи данных, а также одним щелчком мыши запретить сетевую активность.

При весьма миниатюрном размере программа обладает множеством возможностей, часть из которых можно представить так:

- мониторинг любых сетевых интерфейсов и любого сетевого трафика;
- мощная система фильтров, позволяющая оценить объем любой части трафика — вплоть до конкретного сайта в указанном направлении или трафика с каждой машины в локальной сети в указанное время суток;
- неограниченное количество настраиваемых графиков активности сетевых соединений на основе выбранных фильтров;
- управление (ограничение, приостановка) потоком трафика на любом из фильтров;
- удобная система статистики (от часа до года) с функцией экспорта;
- возможность просмотра статистики удаленных компьютеров с BWMeter;
- гибкая система оповещений и уведомлений по достижении определенного события;
- максимальные возможности по настройке, в том числе внешнего вида;
- возможность запуска как сервиса.

Bandwidth Monitor Pro. Её разработчики очень много внимания уделили настройке окна мониторинга трафика. Во-

первых, можно определить, какую именно информацию программа будет постоянно показывать на экране. Это может быть количество полученных и переданных данных (как отдельно, так и в сумме) за сегодня и за любой указанный промежуток времени, среднюю, текущую и максимальную скорость соединения.

Отдельно стоит сказать о системе оповещений, которая удачно реализована. Можно задавать поведение программы при выполнении заданных условий, которыми могут быть передача определенного количества данных за указанный период времени, достижение максимальной скорости загрузки, изменение скорости соединения и пр. Если на компьютере работает несколько пользователей и необходимо следить за общим трафиком, то программу можно запускать как службу. В этом случае Bandwidth Monitor Pro будет собирать статистику всех пользователей, которые заходят в систему под своими логинами.

DUTraffic. От всех программ обзора DUTraffic отличает бесплатный статус. Как и коммерческие аналоги, DUTraffic может выполнять разнообразные действия при выполнении тех или иных условий. Так, например, он может проигрывать аудиофайл, показывать сообщение или же разрывать соединение с Интернетом, когда средняя или текущая скорость загрузки меньше заданного значения, когда продолжительность интернет-сессии превышает указанное число часов, когда передано определенное количество данных. Кроме этого, различные действия могут выполняться циклически, например, каждый раз, когда программа фиксирует передачу заданного объема информации. Статистика в DUTraffic ведется отдельно для каждого пользователя и для каждого соединения с Интернетом. Программа показывает как общую статистику за выбранный промежуток времени, так и информацию о скорости, количестве переданных и принятых данных и финансовых затратах за каждую сессию.

Система мониторинга Cacti. Cacti - это open-source веб-приложение (соответственно отсутствует установочный файл). Cacti собирает статистические данные за определённые временные интервалы и позволяет отобразить их в графическом виде. Система позволяет строить графики при помощи RRDtool. Преимущественно используются стандартные шаблоны для отображения статистики по загрузке процессора, выделению

оперативной памяти, количеству запущенных процессов, использованию входящего/исходящего трафика.

Интерфейс отображения статистики, собранной с сетевых устройств, представлен в виде дерева, структура которого задается самим пользователем. Как правило, графики группируют по определенным критериям, причем один и тот же график может присутствовать в разных ветвях дерева (например, трафик через сетевой интерфейс сервера — в той, которая посвящена общей картине интернет-трафика компании, и в ветви с параметрами данного устройства). Есть вариант просмотра заранее составленного набора графиков, и есть режим предпросмотра. Каждый из графиков можно рассмотреть отдельно, при этом он будет представлен за последние день, неделю, месяц и год. Есть возможность самостоятельного выбора временного промежутка, за который будет сгенерирован график, причем сделать это можно как указав календарные параметры, так и просто выделив мышкой определенный участок на нем.

В табл. 2 представлены сравнительные основные характеристики представленных программ мониторинга сетевого трафика.

Таблица 2. Сравнительные характеристики программ мониторинга сетевого трафика.

Параметр	BM-Extreme	BW-Meter	Bandwidth Monitor Pro	DU-Traffic	Cacti
Размер установочного файла, Мбайт	0,473	1,91	1,05	1,4	–
Язык интерфейса	русский	русский	английский	русский	английский
График скорости	+	–	+	+	–
График трафика	–	+	+	–	+
Экспорт/импорт (формат файла экспорта)	–/–	+/+ (* .csv)	–/–	–/–	+/+ (* .xls)
Запуск мониторинга по требованию	–	+	–	–	+
Минимальный временной шаг между отсчётами данных, с	300	1	60	1	1
Возможность изменения минимального шага между отсчётами данных	+	+	+	–	+

Обзор программ-анализаторов (снифферов) сетевого трафика

Анализатор трафика, или сниффер, — сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа либо только анализа сетевого трафика, предназначенного для других узлов. Анализ прошедшего через сниффер трафика позволяет:

- обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи (снифферы здесь малоэффективны; как правило, для этих целей используют сбор разнообразной статистики серверами и активным сетевым оборудованием и её последующий анализ);
- перехватить любой незашифрованный (а порой и зашифрованный) пользовательский трафик с целью получения паролей и другой информации;
- локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели снифферы часто применяются системными администраторами).

Поскольку в «классическом» сниффере анализ трафика происходит вручную, с применением лишь простейших средств автоматизации (анализ протоколов, восстановление TCP-потока), то он подходит для анализа лишь небольших его объёмов.

Wireshark (ранее — **Ethereal**). Программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Имеет графический пользовательский интерфейс. Wireshark — это приложение, которое «знает» структуру самых различных сетевых протоколов и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня. Поскольку для захвата пакетов используется библиотека Pcap (Packet Capture), существует возможность захвата данных только из тех сетей, которые поддерживаются этой библиотекой. Тем не менее, Wireshark умеет работать с множеством форматов входных данных, соответственно можно открывать файлы данных, захваченных другими программами, что расширяет возможности захвата.

Iris Network Traffic Analyzer (NTA). Помимо стандартных функций сбора, фильтрации и поиска пакетов, а также построения отчетов, программа предлагает уникальные возможности для

реконструирования данных. Iris NTA помогает детально воспроизвести сеансы работы пользователей с различными web-ресурсами и даже позволяет имитировать отправку паролей для доступа к защищенным web-серверам с помощью cookies. Уникальная технология реконструирования данных, реализованная в модуле дешифрования, преобразует сотни собранных двоичных сетевых пакетов в привычные глазу электронные письма, web-страницы, сообщения ICQ и др. eEye Iris позволяет просматривать незашифрованные сообщения web-почты и программ мгновенного обмена сообщениями, расширяя возможности имеющихся средств мониторинга и аудита.

Анализатор пакетов **eEye Iris** позволяет зафиксировать различные детали атаки, такие как дата и время, IP-адреса и DNS-имена компьютеров хакера и жертвы, а также использованные порты.

Ethernet Internet Traffic Statistic (EITS). Эта система показывает количество полученных и принятых данных (в байтах, всего и за последнюю сессию), а также скорость подключения. Для наглядности собираемые данные отображаются в режиме реального времени на графике. Работает без инсталляции, интерфейс — русский и английский. Утилита для контроля степени сетевой активности показывает количество полученных и принятых данных, ведя статистику за сессию, день, неделю и месяц.

CommTraffic (CT) Это сетевая утилита для сбора, обработки и отображения статистики интернет-трафика через модемное (dialup) или выделенное соединение. При мониторинге сегмента локальной сети CommTraffic показывает интернет-трафик для каждого компьютера в сегменте. CommTraffic включает в себя легко настраиваемый, понятный пользователю интерфейс, показывающий статистику работы сети в виде графиков и цифр.

В табл. 3 представлен сравнительный анализ характеристик рассмотренных программ-анализаторов сетевого трафика.

Таблица 3. Сравнительный анализ характеристик программ-анализаторов сетевого трафика

Параметр	Wireshark	Iris NTA	EITS	СТ
Размер установочного файла, Мбайт	17,4	5,04	0,651	7,2
Язык интерфейса	английский	русский	англ./русский	русский
График скорости	+	+	—	—
График трафика	—	—	+	+
Экспорт/импорт (формат файла экспорта)	+/- (*.txt, *.px, *.csv, *.psml, *.pdml, *.c)	-/-	-/-	-/-
Запуск мониторинга по требованию	—	—	—	—
Минимальный шаг между отсчётами данных, с	0,001	1	1	1
Возможность изменения минимального шага между отсчётами данных	+	+	—	—

Получение и подготовка исходных данных для анализа свойств аномалий трафика

В общем виде алгоритм анализа сетевого трафика выглядит следующим образом (рис. 2.2).

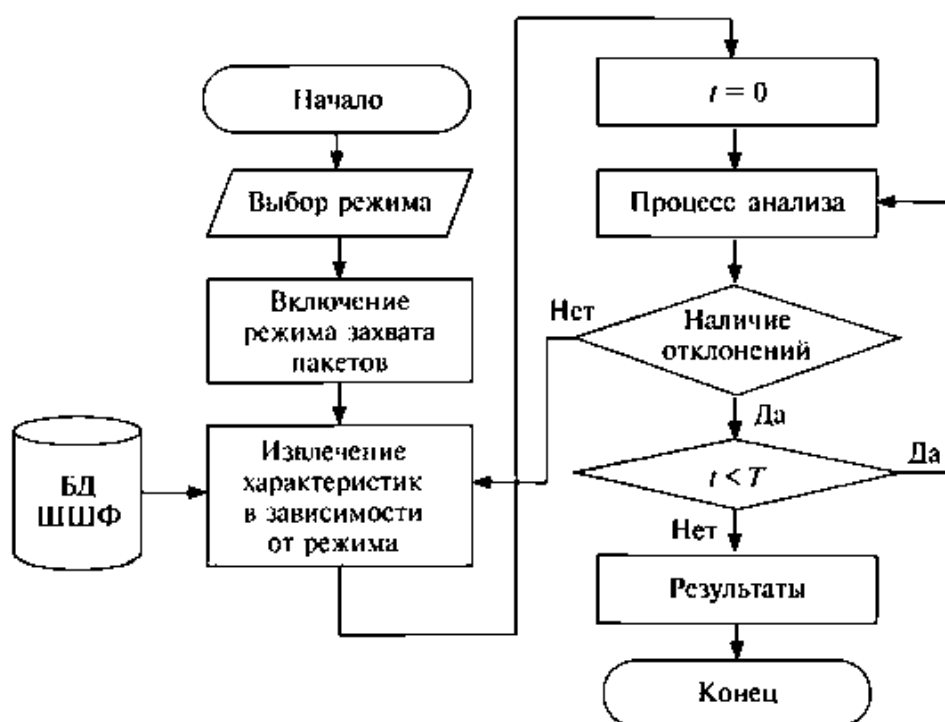


Рис. 2.2. Алгоритм процедуры контроля сети, где БД ШШФ — банк данных шаблонов штатного функционирования сети

При включении режима захвата сетевых пакетов сетевой адаптер переводится в режим Promiscuous и фиксирует любой пакет, прошедший через интерфейс. Это обусловлено технологией передачи информации в сетях Ethernet. Определённые ограничения в режиме анализа дают возможность уменьшить объём анализируемой информации, отсекая излишки неактуальных данных и увеличив быстродействие системы.

В качестве хранилищ используются как SQL-базы данных, так и сформированные двоичные текстовые файлы, хранящие числовые характеристики.

Исходными данными трафика, анализируемого впоследствии на наличие аномалий, предлагается принимать данные, полученные с помощью программы-сниффера Wireshark (или любого другого программного комплекса, осуществляющего задачи снятия дампа сетевой активности).

Программный комплекс Wireshark может использоваться как для записи «живого» трафика с интерфейсов, непосредственно входящих в анализирующую систему, так и для анализа снятого и сохраненного до этого трафика.

TCPdump данные. TCPdump (или Windump для Windows) — популярное и широко применяемое программное средство, позволяющее детально исследовать процесс передачи информации в сети. Вывод tcpdump содержит данные пакетов сетевых соединений в порядке появления пакета в сети. Перед сбором информации данные пакета должны предварительно обрабатываться. Конверторы tcpdump данных преобразовывают записи соединения в множество особенностей (т. е. атрибутов), например, time (стартовое время соединения, т. е. timestamp первого пакета), dur (продолжительность соединения), src и dst (хост источник и адресат), bytes (число байтов данных, отправленных из источника до адресата), sru (сервис, т. е. порт адресата), flag (как соединение соответствует сетевому протоколу) и т. д. Эти существенные особенности суммируют информацию пакетного уровня в пределах соединения.

2.3. Проверка устройств на возможное наличие закладных аппаратных или программных средств компьютерной разведки на критически важных объектах сетевой инфраструктуры России

Проверка объектов критической информационной инфраструктуры (далее - КИИ) России на возможное наличие закладных аппаратных или программных средств компьютерной разведки строится на государственных системах по графику установленному в Политике безопасности, но по индивидуальным запросам, в зависимости от содержания которых, через территориальное подразделение ФСТЭК России в аккредитованные на то ФСТЭКом России организации. Или для коммерческих структур - через правоохранительные органы, которые затем обращаются в территориальное подразделение ФСТЭК России, поручающее такие проверки аккредитованным на то организациям.

В любом из этих случаев работа строится на основании руководящих документов ФСТЭК России, действующих в этот именно период, которые в свою очередь соответствуют действующим государственным стандартам по кругу вопросов выявления и борьбы с программными закладками.

Так, по состоянию на сентябрь 2017 года это Руководящий документ Гостехкомиссии при Президенте России от 04.06.1999г. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей». Действие этого руководящего документа (далее – РД) не распространяется на программное обеспечение (далее – ПО) средств криптографической защиты информации. Документ предназначен для специалистов испытательных лабораторий, заказчиков, разработчиков ПО средств защиты информации (далее – СЗИ). Документ содержит таблицу (см. Таблица 4) требований к уровням контроля отсутствия недеklarированных возможностей (далее - НДВ).

**Таблица 4. Требования к уровням контроля отсутствия
недекларированных возможностей**

Наименование требования	Уровень контроля			
	4	3	2	1
<i>Требования к документации</i>				
1. Контроль состава и содержания документации				
1.1. Спецификация (ГОСТ 19.202–78)	+	=	=	=
1.2. Описание программы (ГОСТ 19.402–78)	+	=	=	=
1.3. Описание применения (ГОСТ 19.502–78)	+	=	=	=
1.4. Пояснительная записка (ГОСТ 19.404–79)	–	+	=	=
1.5. Тексты программ, входящих в состав ПО (ГОСТ 19.401–78)	+	=	=	=
<i>Требования к содержанию испытаний</i>				
2. Контроль исходного состояния ПО	+	=	=	=
3. Статический анализ исходных текстов программ				
3.1. Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
3.2. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	+	=	=	+
3.3. Контроль связей функциональных объектов по управлению	–	+	=	=
3.4. Контроль связей функциональных объектов по информации	–	+	=	=
3.5. Контроль информационных объектов	–	+	=	=
3.6. Контроль наличия заданных конструкций в исходных текстах	–	–	+	+
3.7. Формирование перечня маршрутов выполнения функциональных объектов	–	+	+	=
3.8. Анализ критических маршрутов выполнения функциональных объектов	–	–	+	=
3.9. Анализ алгоритма работы функциональных объектов на основе блок-схем, диаграмм и т. п., построенных по исходным текстам контролируемого ПО	–	–	+	=
4. Динамический анализ исходных текстов программ				
4.1. Контроль выполнения функциональных объектов	–	+	+	=
4.2. Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	–	+	+	=
5. Отчетность	+	+	+	+

Среди действующих документов в области защиты КИИ от программных закладок, использующих так называемые «скрытые

каналы», следует также отметить два национальных стандарта Российской Федерации:

- ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения»;

- ГОСТ Р 53113.2-2009 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов».

Развитие, внедрение и использование распределенных информационных систем и технологий, использование импортных программно-аппаратных средств привели к появлению класса угроз информационной безопасности, связанных с использованием так называемых скрытых информационных каналов (далее - СК), невидимых для традиционных средств защиты информации.

Традиционные средства обеспечения ИБ, такие как средства разграничения доступа, межсетевые экраны, системы обнаружения вторжений, контролируют только информационные потоки, которые проходят по каналам, предназначенным для их передачи. Возможность обмена информацией вне этих рамок посредством скрытых каналов не учитывается. Опасность СК для информационных технологий и автоматизированных систем и других активов организации связана с отсутствием контроля средствами защиты информационных потоков, что может привести к утечке информации и нарушить целостность информационных ресурсов и программного обеспечения в компьютерных системах.

СК используются для систематического взаимодействия вредоносных программ (компьютерных вирусов) с нарушителем безопасности при организации атаки на АС, которая не обнаруживается средствами контроля и защиты. Опасность СК основана на предположении о том, что нарушитель имеет постоянный доступ к информационным ресурсам и возможность воздействовать через эти каналы на информационную систему для нанесения максимального ущерба.

Для обеспечения защиты информации, обрабатываемой в АС, необходимо выявлять и нейтрализовывать все возможные информационные каналы несанкционированного действия, в том числе скрытые.

Существенным моментом защищенности систем ИТ и АС является доверие к системам защиты. В системах, требующих обеспечения повышенного уровня доверия, должны учитываться угрозы безопасности, возникающие вследствие наличия возможности несанкционированного действия с помощью СК. Требования доверия к безопасности информации установлены в ГОСТ Р ИСО/МЭК 15408-3, в соответствии с которым для систем с оценочным уровнем доверия, начиная с ОУД5, предусмотрено проведение обязательного анализа СК. Таким образом, требование анализа СК в Российской Федерации является необходимым условием безопасного функционирования систем, обрабатывающих ценную информацию или использующих импортное аппаратно-программное обеспечение.

Стандарт ГОСТ Р 53113.1-2008 устанавливает классификацию СК, определяет задачи, решаемые при проведении анализа СК, а также устанавливает порядок проведения анализа для ИТ и АС. Он предназначен для использования заказчиками, разработчиками и пользователями ИТ при формировании ими требований к разработке, приобретению и применению продуктов и систем ИТ, которые предназначены для обработки, хранения или передачи информации, подлежащей защите. Стандарт предназначен также для использования органами сертификации и испытательными лабораториями при оценке безопасности и сертификации безопасности ИТ и АС.

Стандарт определяет следующий порядок действий (этапы) по определению степени опасности СК для активов организации, выявлению и противодействию СК:

- классификация активов в зависимости от степени опасности атак с использованием СК с учетом возможных угроз безопасности активам и анализ рисков;
- анализ СК, включающий в себя их идентификацию (определение источника и получателя) и оценку опасности, которую несет их скрытое функционирование;

- реализация мероприятий по защите от угроз, реализуемых с использованием СК;
- организация контроля противодействия СК.

Противодействие опасным СК может осуществляться с помощью следующих средств и методов:

- построение архитектуры ИТ или АС, позволяющей перекрыть СК или сделать их пропускную способность настолько низкой, что каналы становятся неопасными;
- использование технических средств, позволяющих перекрывать СК или снижать их пропускную способность до уровня, ниже заданного;
- использование программно-технических средств, позволяющих выявлять работу опасных СК в процессе эксплуатации системы;
- применение организационно-технических мер, позволяющих ликвидировать СК или уменьшить их пропускную способность до безопасного значения.

Угрозы безопасности, которые могут быть реализованы с помощью СК, включают в себя:

- внедрение вредоносных программ и данных;
- подачу злоумышленником команд агенту для выполнения;
- утечку криптографических ключей или паролей;
- утечку отдельных информационных объектов.

Системами, наиболее сильно подверженными атакам с использованием СК, являются:

- многопользовательские распределенные системы;
- системы с выходом в глобальные сети;
- системы, использующие криптографические средства защиты;
- системы, использующие многоуровневую (мандатную) политику разграничения доступа;
- системы, программно-аппаратные агенты в которых не могут быть обнаружены (в связи с использованием программного и аппаратного обеспечения с недоступным исходным кодом и в связи с отсутствием конструкторской документации).

В зависимости от степени опасности атак с использованием СК защищаемые активы организации подразделяют на следующие классы:

- 1-й класс — активы, содержащие информацию, степень подверженности которой атакам, реализуемым с использованием СК, определяет собственник;

- 2-й класс — активы, содержащие информацию ограниченного доступа или персональные данные и обрабатываемые в системах, имеющих технические интерфейсы с открытыми сетями или компьютерными системами общего доступа, а также компьютерными системами, не предполагающими защиту от утечки по техническим каналам;

- 3-й класс — активы, содержащие сведения, составляющие государственную тайну.

Кроме того, существует особый класс активов, которые уязвимы с точки зрения угроз, реализуемых с использованием СК с низкой пропускной способностью:

- класс А — активы, связанные с функционированием критически важных объектов;

- класс Б — активы, содержащие ключевую/парольную информацию, в том числе ключи криптографических систем защиты информации и пароли доступа к иным активам.

В стандарте ГОСТ Р 53113.2-2009 установлены подробные рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов в соответствии с этапами, определенными в первой части стандарта. Он предназначен как для заказчиков, разработчиков и пользователей информационных технологий (далее –ИТ) в процессе формирования требований по защите информации на стадиях разработки, приобретения и применения ИТ-продуктов и автоматизированных систем (далее – АС) в соответствии с требованиями нормативных правовых документов, так и для органов сертификации и испытательных лабораторий при проведении подтверждения соответствия ИТ и АС требованиям к обеспечению безопасности информации.

Стандарт устанавливает типовой порядок организации противодействия СК, который может уточняться с учетом условий и особенностей применения информационных технологий в АС.

Организация защиты ИТ и АС от атак с использованием СК включает в себя процедуры их выявления и подавления. Набор применяемых методов выявления и/или подавления СК должен определяться исходя из модели угроз безопасности организации. Мероприятия по защите от атак с использованием СК должны быть интегрированы в систему информационной безопасности организации.

Результаты любых таких проверок и изучения ИС на предмет наличия программных закладок и/или скрытых каналов оформляются актом в 3-х экземплярах, один из которых хранится в аккредитованной ФСТЭК России организации вместе с экземпляром контракта со ФСТЭК России, второй – во ФСТЭК России с их экземпляром контракта и запросом «с места проверки», третий остается в организации, эксплуатирующей КИИ, для учета результатов проверки в коррекции политики безопасности.

Контрольные вопросы:

1. Охарактеризуйте «эксплойты», вредоносные программы и методы доведения сервисов до «отказа в обслуживании», которые используются для проведения компьютерной разведки?
2. Какие модели компьютерных атак приводятся в литературе?
3. Какие этапы реализации атак приводятся в литературе?
4. Как осуществляется сбор информации перед атакой в интересах компьютерной разведки?
5. Назовите и охарактеризуйте основные механизмы реализации компьютерных атак.
6. Назовите известные вам программы анализа мониторинга сетевого трафика (снифферов) и охарактеризуйте особенности их работы?
7. Назовите и охарактеризуйте применяемые в России методы проверки аппаратно-программных решений на наличие программных и аппаратных закладок, предусмотренных для критически важных объектов сетевой инфраструктуры России.

Задания для самостоятельной работы к главе 2:

Вариант № 1. Привести примеры программ-анализаторов сетевого трафика, которые можно использовать в интересах

выявления признаков и фактов проведения компьютерной разведки.

Вариант № 2. Как производится получение и подготовка исходных данных для анализа сетевого трафика на аномалии, подозрительные на применение средств компьютерной разведки?

Вариант № 3. Указать и обосновать критерии аномального поведения сетевого трафика, подозрительного на проведение компьютерной разведки.

3. Оценка уязвимости систем для компьютерной разведки

Особенности использования в России методов выявления уязвимости объектов информатизации для средств проведения компьютерной разведки заключаются в том, что идентификация уязвимостей входит в четвертый шаг первого подэтапа оценки рисков, предусмотренной серией международных и российских стандартов семейства 27000 (а именно ГОСТ Р ИСО/МЭК 27005-2010). А структура и содержание описания уязвимостей, их классификация предусмотрены стандартами ГОСТ Р 56545-2015 и 56546-2015. Потребовалось почти пять лет для того, чтобы «разобраться» с мировыми требованиями и адаптировать их к российским условиям и быстро меняющейся нормативной базе в сфере информационной безопасности (далее - ИБ).

3.1. Выявление уязвимости объектов информатизации для средств проведения компьютерной разведки

Согласно ГОСТ Р ИСО/МЭК 27005-2010 и ISO/IEC 27005:2011 входными данными являются списки известных угроз ИБ, защищаемых активов и существующих средств управления. На этом шаге идентифицируются уязвимости, которые могут быть использованы угрозами ИБ (точнее источниками угроз ИБ) для причинения ущерба активам или всей организации в целом, в том числе и методами КР.

Существует несколько разных классификаций уязвимостей: по причинам возникновения, по месту нахождения, по степени

критичности последствий от ее использования угрозами ИБ, а также по вероятности реализации.

По причинам возникновения уязвимости подразделяются на три класса:

- проектирования, использующие анализ алгоритма ПО и АО;
- реализации, использующие анализ исходного текста (его синтаксиса, семантики, конструкций и т. п.) или исполняемого файла (его атрибутов, процесса выполнения - операции с памятью, работа с указателями, вызов функций), внешними воздействиями, когда на вход подаются разные граничные и маловероятные значения переменных, а также дизассемблированием и анализом полученного кода;
- эксплуатации, включая слабости системной политики, ошибки настройки ПО и АО и пр.

По месту нахождения уязвимости могут быть идентифицированы в следующих областях:

- организация в целом;
- ее процессы и процедуры (организация работ);
- установившаяся практика (порядок) управления и администрирования;
- персонал;
- физическая среда;
- конфигурации ИС;
- аппаратное, программное и телекоммуникационное оборудование;
- зависимость от внешних сторон.

Уязвимость может присутствовать в активе, а может находиться и в средстве обеспечения его ИБ. Также выделяют уязвимости на уровне сети, отдельного хоста (устройства с уникальным адресом) или приложения.

По степени критичности (уровню риска) уязвимости делятся следующим образом (при этом уровень риска (англ. level of risk) - это величина риска или комбинации рисков, выраженная как сочетание последствий и возможности их возникновения):

- высокий уровень риска - уязвимости, позволяющие атакующему получить доступ к хосту с правами

суперпользователя, а также уязвимости, делающие возможным обход средств защиты для попадания в Интранет организации;

- средний уровень риска - уязвимости, позволяющие атакующему получить информацию, которая с высокой степенью вероятности позволит получить доступ к отдельному хосту и уязвимости, приводящие к повышенному расходу ресурсов системы (за счет атак «отказ в обслуживании»);

- низкий уровень риска - уязвимости, позволяющие осуществлять сбор критической информации о системе (например, неиспользуемые службы, текущее время на компьютере для последующих атак на криптоалгоритмы и т. д.).

Уязвимости можно оценить по вероятности реализации на ее основе угрозы ИБ:

- высоковероятная или вероятная - данную уязвимость легко использовать, защита отсутствует или очень слаба;

- возможная - уязвимость может быть использована, но имеется защита;

- маловероятная или невозможная - данную уязвимость использовать трудно, имеется хорошая защита.

Сама по себе уязвимость (просто ее наличие) не причиняет вреда - для этого нужны угроза ИБ и ее источник, которые ею воспользуются. Уязвимость лишь создает потенциальные условия для реализации угрозы ИБ.

Уязвимость, для которой не выявлено соответствующей угрозы ИБ, может и не требовать реализации средств управления, но она все равно должна быть осознана и должен осуществляться мониторинг ее изменений. И наоборот, угроза ИБ, для реализации которой в системе нет уязвимости, не актуальна для этой системы и не влечет за собой риска ИБ.

Следует отметить, что некорректная реализация или использование и неправильное функционирование средств управления и, следовательно, защитных мер (например, при некорректной конфигурации) могут также создать уязвимость. Средство управления может быть эффективным или неэффективным в зависимости от среды его функционирования.

Уязвимости могут быть связаны со свойствами актива. Способ и цели использования актива могут отличаться от планируемых при его приобретении или создании. Необходимо

учитывать уязвимости различного происхождения, например, внутренние или внешние по отношению к данному активу.

Примеры уязвимостей применительно к различным объектам, требующим ОИБ, приведены далее (см. Примеры уязвимостей).

Выходными данными процесса являются два списка - уязвимости по отношению к активам, угрозам ИБ и средствам управления и уязвимости, не связанные ни с какими обнаруженными угрозами ИБ.

Примеры уязвимостей:

1. Среда и инфраструктура:

- отсутствие физической защиты зданий, дверей и окон (возможна, например, угроза кражи);
- неправильное или халатное использование физических средств управления доступом в здания, помещения (возможна, например, угроза намеренного повреждения);
- нестабильная работа электросети (возможна, например, угроза колебаний напряжения);
- размещение в зонах возможного затопления (возможна, например, угроза затопления) и т. д.

2. Аппаратное обеспечение (далее – АО):

- отсутствие схем периодической замены (возможна, например, угроза ухудшения состояния запоминающей среды);
- подверженность колебаниям напряжения (возможна, например, угроза возникновения колебаний напряжения);
- подверженность температурным колебаниям (возможна, например, угроза возникновения экстремальных значений температуры);
- подверженность воздействию влаги, пыли, загрязнения (возможна, например, угроза запыления);
- чувствительность к воздействию электромагнитного излучения (возможна, например, угроза воздействия электромагнитного излучения);
- недостаточное обслуживание/неправильная установка запоминающих сред (возможна, например, угроза возникновения ошибки при обслуживании);

- отсутствие контроля за эффективным изменением конфигурации (возможна, например, угроза ошибки операторов) и т. д.

3. ПО:

- неясные или неполные технические требования к разработке средств ПО (возможна, например, угроза программных сбоев);

- отсутствие тестирования или недостаточное тестирование ПО (возможна, например, угроза использования ПО несанкционированными пользователями);

- сложный пользовательский интерфейс (возможна, например, угроза ошибки операторов);

- отсутствие механизмов идентификации и аутентификации, например, аутентификации пользователей (возможна, например, угроза нелегального проникновения злоумышленников под видом законных пользователей);

- отсутствие аудиторской проверки (возможна, например, угроза использования ПО несанкционированным способом);

- хорошо известные дефекты ПО (возможна, например, угроза использования ПО несанкционированными пользователями);

- незащищенные таблицы паролей (возможна, например, угроза нелегального проникновения злоумышленников под видом законных пользователей);

- плохое управление паролями (легко определяемые пароли, хранение в незашифрованном виде, недостаточно частая замена паролей);

- неправильное присвоение прав доступа (возможна, например, угроза использования ПО несанкционированным способом);

- неконтролируемая загрузка и использование ПО (возможна, например, угроза столкновения с вредоносным ПО);

- отсутствие регистрации конца сеанса при выходе с рабочей станции (возможна, например, угроза использования ПО несанкционированными пользователями);

- отсутствие эффективного контроля внесения изменений (возможна, например, угроза программных сбоев);

- отсутствие документации (возможна, например, угроза ошибки операторов);
- отсутствие резервных копий (возможна, например, угроза воздействия вредоносного ПО или пожара);
- списание или повторное использование запоминающих сред без надлежащего стирания записей (возможна, например, угроза использования ПО несанкционированными пользователями);
- отсутствие процедуры контроля изменений и т. д.

4. Коммуникации:

- незащищенные линии связи (возможна, например, угроза перехвата информации);
- неудовлетворительная стыковка кабелей (возможна, например, угроза несанкционированного проникновения к средствам связи);
- отсутствие идентификации и аутентификации отправителя и получателя (возможна, например, угроза нелегального проникновения злоумышленников под видом законных пользователей);
- пересылка паролей открытым текстом (возможна, например, угроза доступа несанкционированных пользователей к сети);
- отсутствие подтверждений отправки или получения сообщения (возможна, например, угроза изменения смысла переданной информации);
- коммутируемые линии (возможна, например, угроза доступа несанкционированных пользователей к сети);
- незащищенные потоки конфиденциальной информации (возможна, например, угроза перехвата информации);
- неадекватное управление сетью, недостаточная гибкость маршрутизации (возможна, например, угроза перегрузки трафика);
- незащищенные подключения к сетям общего пользования (возможна, например, угроза использования ПО несанкционированными пользователями) и т. д.

5. Документы:

- хранение в незащищенных местах (возможна, например, угроза хищения);

- недостаточная внимательность при уничтожении (возможна, например, угроза хищения);
- бесконтрольное копирование (возможна, например, угроза хищения) и т. д.

6. Персонал:

- отсутствие персонала (возможна, например, угроза недостаточного числа работников);
- отсутствие надзора за работой лиц, приглашенных со стороны, или за работой уборщиц (возможна, например, угроза хищения);
- недостаточная подготовка персонала по вопросам обеспечения ИБ (возможна, например, угроза ошибки операторов);
- отсутствие необходимых знаний по вопросам ИБ (возможна, например, угроза ошибок пользователей);
- неправильное использование программно-аппаратного обеспечения (возможна, например, угроза ошибки операторов);
- отсутствие механизмов отслеживания (возможна, например, угроза использования ПО несанкционированным способом);
- отсутствие политики правильного пользования телекоммуникационными системами для обмена сообщениями (возможна, например, угроза использования сетевых средств несанкционированным способом);
- несоответствующие процедуры набора кадров (возможна, например, угроза намеренного повреждения);
- неадекватная ответственность за техническое обслуживание;
- отсутствие надлежащего распределения обязанностей за ОИБ и т. д.

7. Общие уязвимые места:

- отказ системы вследствие отказа одного из элементов (возможна, например, угроза сбоев в функционировании услуг связи);
- неадекватные результаты проведения технического обслуживания (возможна, например, угроза аппаратных отказов);
- отсутствие или недостаточные условия, касающиеся ИБ, в договорах с клиентами и/или третьими лицами;
- отсутствие регулярных аудитов;

- отсутствие или неудовлетворительное соглашение об уровне сервисов;
- отсутствие планов ОНБ;
- отсутствие оговоренного дисциплинарного процесса в случае инцидента ИБ и т. д.

Стандарты по уязвимостям ИС (ГОСТ Р 56545-2015 и 56546-2015) введены в действие 1.04.2016г.

Структура и содержание описания уязвимостей в ГОСТ Р 56545-2015. В стандарте приняты следующие понятия и определения.

Уязвимость: Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использован(а) для реализации угроз безопасности информации.

Правила описания уязвимости: Совокупность положений, регламентирующих структуру и содержащих описания уязвимости.

Описание уязвимости: Информация о выявленной уязвимости.

Паспорт уязвимости: Документ (формализованное представление), содержащий описание уязвимости, определяющий характеристики уязвимости и выполненный в соответствии с правилами описания уязвимости.

Известная уязвимость: Уязвимость, опубликованная в общедоступных источниках с описанием соответствующих мер защиты информации, исправлений недостатков или соответствующих обновлений.

Впервые выявленная уязвимость: Уязвимость, не опубликованная в общедоступных источниках.

Уязвимость нулевого дня: Уязвимость, которая становится известной до момента выпуска разработчиком компонента информационной системы соответствующих мер защиты информации, исправлений мед остатков или соответствующих обновлений.

Общие требования к структуре описания уязвимости

Структура описания уязвимости должна обеспечивать достаточность информации для идентификации уязвимости ИС и выполнения работ по анализу уязвимостей ИС.

Для однозначной идентификации уязвимости описание должно включать следующие элементы:

- идентификатор уязвимости;
- наименование уязвимости;
- класс уязвимости;
- наименование программного обеспечения (ПО) и его версии.

Для обеспечения работ по анализу уязвимостей ИС описание должно включать следующие элементы:

- идентификатор типа недостатка;
- тип недостатка;
- место возникновения (проявления) уязвимости;
- способ (правило) обнаружения уязвимости;
- возможные меры по устранению уязвимости.

Для обеспечения детальной информации об уязвимости описание может включать следующие элементы:

- наименование операционной системы и тип аппаратной платформы;
- язык программирования ПО;
- служба (порт), которую(ый) используют для функционирования ПО;
- степень опасности уязвимости;
- краткое описание уязвимости;
- идентификаторы других систем описаний уязвимостей;
- дата выявления уязвимости;
- автор, опубликовавший информацию о выявленной уязвимости;
- критерии опасности уязвимости.

Дополнительно описание уязвимости ИС может включать прочую информацию в составе следующих элементов:

- описание реализуемой технологии обработки (передачи) информации;
- описание конфигурации ПО, определяемой параметрами установки;
- описание настроек ПО, при которых выявлена уязвимость;
- описание полномочий (прав доступа) к ИС, необходимых нарушителю для эксплуатации уязвимости;
- описание возможных угроз безопасности информации, реализация которых возможна при эксплуатации уязвимости;

- описание возможных последствий от эксплуатации уязвимости ИС;
- наименование организации, которая опубликовала информацию о выявленной уязвимости;
- дата опубликования уведомления о выявленной уязвимости, а также дата устранения уязвимости разработчиком ПО;
- другие сведения.

Далее в стандарте приводится разъяснение по каждому из этих пунктов и примеры описания уязвимостей.

Новая классификация уязвимостей по ГОСТ Р 56546-2015:

В стандарте приняты следующие понятия и определения.

1.1 Угроза безопасности информации: Совокупность условия и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

1.2 Уязвимость кода: Уязвимость, появившаяся в процессе разработки программного обеспечения.

1.3 Уязвимость конфигурации: Уязвимость, появившаяся в процессе задания конфигурации (применения параметров настройки) программного обеспечения и технических средств информационной системы.

1.4 Уязвимость архитектуры: Уязвимость, появившаяся в процессе проектирования информационной системы.

1.5 Уязвимость организационная: Уязвимость, появившаяся в связи с отсутствием (или недостатками) организационных мер защиты информации в информационной системе и (или) несоблюдением правил эксплуатации системы защиты информации информационной системы, требований организационно-распорядительных документов по защите информации и (или) несвоевременном выполнении соответствующих действий должностным лицом (работником) или подразделением, ответственными за защиту информации.

1.6 Уязвимость многофакторная: Уязвимость, появившаяся в результате наличия нескольких недостатков различных типов.

1.7 Язык программирования: Язык, предназначенный для разработки (представления) программного обеспечения.

1.8 Степень опасности уязвимости: Мера (сравнительная величина), характеризующая подверженность информационной

системы уязвимости и ее влияние на нарушение свойств безопасности информации (конфиденциальность, целостность, доступность).

В основе классификации уязвимостей ИС используются следующие классификационные признаки:

- **область происхождения уязвимости;**
- **типы недостатков ИС;**
- **место возникновения (проявления) уязвимости ИС.**

Помимо классификационных признаков уязвимостей ИС используются поисковые признаки (основные и дополнительные). Поисковые признаки предназначены для организации расширенного поиска в базах данных уязвимостей.

К основным поисковым признакам уязвимостей ИС относятся следующие:

- наименование операционной системы (ОС) и тип аппаратной платформы;
- наименование программного обеспечения (ПО) и его версия;
- степень опасности уязвимости.

К дополнительным поисковым признакам уязвимостей ИС относятся следующие:

- язык программирования;
- служба (порт), которая (который) используется для функционирования ПО.

Классификация уязвимостей

Уязвимости ИС по области происхождения подразделяются на следующие классы:

- уязвимости кода;
- уязвимости конфигурации;
- уязвимости архитектуры;
- организационные уязвимости;
- многофакторные уязвимости.

Типы недостатков ИС:

- недостатки, связанные с неполнотой проверки вводимых (входных) данных;
- недостатки, связанные с возможностью прослеживания пути доступа к каталогам;
- недостатки, связанные с возможностью перехода по ссылкам;

- недостатки, связанные с возможностью внедрения команд ОС;
 - недостатки, связанные с межсайтовым скриптингом (выполнением сценариев);
 - недостатки, связанные с внедрением интерпретируемых операторов языков программирования или разметки;
 - недостатки, связанные с внедрением произвольного кода;
 - недостатки, связанные с переполнением буфера памяти.
- недостатки, связанные с неконтролируемой форматной строкой;
- недостатки, связанные с вычислениями.

К недостаткам, связанным с вычислениями относятся следующие:

- некорректный диапазон, когда ПО использует неверное максимальное или минимальное значение, которое отличается от верного на единицу в большую или меньшую сторону;
- ошибка числа со знаком, когда нарушитель может ввести данные, содержащие отрицательное целое число, которые программа преобразует в положительное нецелое число;
- ошибка усечения числа, когда часть числа отсекается (например, вследствие явного или неявного преобразования или иных переходов между типами чисел);
- ошибка индикации порядка байтов в числах, когда в ПО смешивается порядок обработки битов (например, обратный и прямой порядок битов), что приводит к неверному числу в содержимом, имеющем критическое значение для безопасности;
- недостатки, приводящие к утечке/раскрытию информации ограниченного доступа.

Утечка информации - это преднамеренное или неумышленное разглашение информации ограниченного доступа (например, существует утечки информации при генерировании ПО сообщения об ошибке, которое содержит сведения ограниченного доступа). Недостатки, приводящие к утечке/раскрытию информации ограниченного доступа, могут быть образованы вследствие наличия иных ошибок (например, ошибок, связанных с использованием скриптов):

- недостатки, связанные с управлением полномочиями (учетными данными);
- недостатки, связанные с управлением разрешениями, привилегиями и доступом;
- недостатки, связанные с аутентификацией;

- недостатки, связанные с криптографическими преобразованиями (недостатки шифрования);
- недостатки, связанные с подменой межсайтовых запросов;
- недостатки, приводящие к «состоянию гонки»;
- недостатки, связанные с управлением ресурсами;
- иные типы недостатков.

Уязвимости ИС по месту возникновения (проявления) подразделяются на следующие:

- уязвимости в общесистемном (общем) программном обеспечении;
- уязвимости в прикладном программном обеспечении;
- уязвимости в специальном программном обеспечении;
- уязвимости в технических средствах;
- уязвимости в портативных технических средствах;
- уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании;
- уязвимости в средствах защиты информации.

3.2. Оценка эффективности принимаемых защитных мер

Оценка эффективности принимаемых защитных мер, против КР в том числе, определяется по международному стандарту ISO/IEC 27004:2009 и национальному стандарту ГОСТ Р ИСО/МЭК 27004-2011.

Стандарт ISO/IEC 27004:2009 «Information technology. Security techniques. Information security management. Measurement» («Информационная технология. Методы и средства обеспечения безопасности. Менеджмент ИБ. Измерение») предназначен для помощи организациям в оценке результативности деятельности по управлению ИБ в рамках имеющихся у них систем управления информационной безопасностью (далее - СУИБ) за счет предоставления единого руководства по применению механизмов получения оценки в результате измерений и введения показателей. На основе полученных показателей, их анализа и принятия соответствующих решений по устранению выявленных проблем организациям удастся повысить результативность функционирования их СУИБ. Эта информация крайне важна для обоснования всех решений, связанных с СУИБ, при внедрении

СУИБ и необходимости внесения изменений в существующую СУИБ для ее дальнейшего совершенствования (улучшения).

С января 2012 г. в России введен в действие ГОСТ Р ИСО/МЭК 27004-2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения», идентичный ISO/IEC 27004:2009. В стандарте содержатся общее руководство, рекомендации по разработке и использованию измерений, мер измерений и их сбору для оценки эффективности и результативности внедренной в организации СУИБ, а также мерам и средствам управления ИБ (и их группам), определенным в ISO/IEC 27001, включая политику, управление рисками ИБ, задачи средств управления, сами средства управления, процессы и процедуры, поддержку процесса их пересмотра, помощь в определении необходимости изменения или совершенствования процессов или средств управления СУИБ.

ГОСТ Р ИСО/МЭК 27004-2011 содержит следующие основные разделы:

- 1) обзор измерений, связанных с ИБ (цели, программа, факторы успеха, модель измерений);
- 2) обязанности руководства;
- 3) разработка методов и мер измерений (процессов их сбора и показателей);
- 4) процесс измерений;
- 5) анализ данных и отчетность по результатам измерений;
- 6) оценивание и совершенствование программы измерений в организации.

В приложениях к стандарту предложен шаблон (типовая форма) описания измерений и приведены некоторые рабочие примеры.

ГОСТ Р ИСО/МЭК 27004-2011 подразумевает, что начальной точкой для разработки измерений и мер измерений является правильное понимание организацией рисков ИБ, с которыми она сталкивается, и того, что деятельность в данном направлении осуществляется корректно (например, на основе ISO/IEC 27005), как того требует ISO/IEC 27001. Для проведения данных мероприятий требуется разработка программы измерений, связанных с ИБ. Полученные во время измерений результаты позволят выявить прогресс (или отсутствие такового) в

достижении целей оценки информационной безопасности (далее – ОИБ) за некоторый период времени как одного из элементов процесса непрерывного совершенствования СУИБ организации.

Стандарт содержит достаточно детальное описание процессов измерения, использование операции агрегирования полученных мер измерений, математического вычисления производных (от двух и более основных) мер и последующего применения аналитических методов и методов принятия решений для выявления «индикаторов» совершенствования СУИБ. Но, к сожалению, не указывается, какие именно основные и производные меры измерений и индикаторы могут на практике наилучшим образом повлиять на это совершенствование.

Само измерение определяется как процесс получения информации об эффективности СУИБ и элементах управления ИБ с использованием метода измерения, функций измерения, аналитической модели и критериев принятия решений.

Механизмы, описанные в стандарте, применимы к различным организациям с различными СУИБ. Подход организации для выполнения требований к измерениям, определенным в ISCMEC 27001, зависит от ряда существенных факторов, включая риски ИБ, величину организации, имеющиеся ресурсы и применимые правовые, нормативные и договорные требования. Рациональный подход важен для обеспечения того, чтобы для этой деятельности СУИБ не выделялись чрезмерные ресурсы в ущерб другой необходимой деятельности. В идеальном случае текущая деятельность, связанная с постоянными измерениями, должна быть интегрирована в обычную деятельность организации с привлечением минимальных дополнительных ресурсов.

Для организаций небольшого размера число мер измерений может быть невелико и для них необходимо разработать одну программу измерений, в то время как для крупных организаций таких программ может быть создано несколько.

На основе ГОСТ Р ИСО/МЭК 27004-2011 организация сможет разработать для себя документацию, которая будет свидетельствовать, что в ней ведется контроль за ОИБ и производится его всесторонняя оценка.

3.3. Дополнительный анализ истории и содержания инцидентов безопасности (по материалам аналитического отчета InfoWatch)

Аналитический центр известной российской компания InfoWatch (www.infowatch.ru/analytics) раз в полгода (ежегодно дважды) публикует доклад с анализом состава и направленности инцидентов безопасности в мире.

Так, в 2016 году в мире было обнародовано (в СМИ и иных источниках) и зарегистрировано Аналитическим центром InfoWatch 1556 случаев утечки конфиденциальной информации, что на 3,4% превышает количество утечек, зарегистрированных в 2015 году. Внешние атаки стали причиной 38% случаев утечек данных. Доля утечек информации вследствие внешних атак выросла на шесть процентных пунктов (п. п.) по сравнению с аналогичным показателем 2015 года. 93% утечек были связаны с компрометацией персональных данных и платежной информации. Всего за исследуемый период было скомпрометировано более 3,1 млрд записей — в три раза больше, чем было зафиксировано в 2015 году. В 2016 году было зафиксировано 44 «мега-утечки», в результате каждой из которых «утекло» не менее 10 млн единиц персональных данных. Совокупно на «мега-утечки» пришлось 94,6% всех скомпрометированных записей. В 36% случаев виновными в утечке информации оказывались сотрудники, а в 2,2% случаев — высшие руководители организаций. По итогам 2016 года Россия заняла второе место в мире по числу известных случаев утечек. В исследуемый период было зарегистрировано 213 случаев утечки конфиденциальной информации из российских коммерческих и государственных организаций. Число «российских» утечек по сравнению с данными 2015 года выросло на 80%.

Аннотация

Аналитический центр компании InfoWatch представляет ежегодный отчет об исследовании утечек конфиденциальной информации.

В 2016 году мы впервые столкнулись с системными проявлениями «политического хактивизма». В результате взломов были похищены десятки миллионов данных филиппинских,

мексиканских, турецких, американских избирателей. Непрерывные скандалы, связанные с утечкой данных, сопровождали предвыборную гонку нынешнего президента США и, возможно, решили ее исход.

Внешние атаки стали причиной компрометации данных пользователей онлайн- платформ Facebook, Foursquare, GitHub, iCloud, LinkedIn, MySpace, Snapchat, Telegram, Tumblr, Twitter. Сложно назвать хотя бы один интернет-сервис, чьи пользователи в 2016 году не пострадали от действий внешних или внутренних злоумышленников.

Любая крупная компания с «громким» именем гарантированно «получает» первые полосы в СМИ в случае, если есть хоть малейший намек на утечку данных по ее вине. В этом году такого внимания удостоились Alibaba, AliExpress, Amazon, American Express, Apple, AT&T, Baidu, BMW, Cisco, Credit Suisse, Dell, Deutsche Telekom, Experian, Google, Huawei, владельцы сети отелей Hyatt и Marriott, KFC, Microsoft, Nokia, Oracle, T-Mobile, Toyota, Uber, Valve, Vodafone, Walmart, Yahoo.

Масштабы утечек и, как следствие, сопутствующих финансовых потерь поистине огромны — по данным компании FireEye, только на участников одной хакерской группировки FIN6 пришлось компрометация 20 млн кредитных карт, что принесло хакерам более 400 млн долл. США.

Не обошла беда и правительственные учреждения, администрации регионов, министерства и ведомства, включая силовые, полицейские структуры. Утечки данных были зарегистрированы в Госдепартаменте и Олимпийском комитете США, в американской налоговой службе, в предвыборных штабах Дональда Трампа и Хиллари Клинтон.

Общемировой тренд увеличения числа утечек информации и объемов скомпрометированных данных определяется не особенностями того или иного региона, а новыми возможностями, которые связаны с использованием информации в цифровом мире, включая перевод услуг в электронный вид, e-commerce, электронную валюту, интеллектуальную собственность в цифровом виде.

Очевидно, что чем больше появляется таких возможностей, тем выше становится интерес злоумышленников к цифровым

данным. Анализ утечек данных на глобальной выборке дает наглядное представление о сегодняшней картине угроз, связанных с компрометацией данных. Например, о том, какой канал более других уязвим в настоящее время и почему, какую отрасль злоумышленники считают наиболее привлекательной и что опаснее — внешняя атака или действия злонамеренного инсайдера.

Методология

Исследование проводится на основе собственной базы данных, пополняемой специалистами Аналитического центра InfoWatch с 2004 года. В базу попадают публичные сообщения о случаях утечки информации из коммерческих, некоммерческих (государственных, муниципальных) организаций, госорганов, которые произошли вследствие умышленных или неосторожных действий сотрудников и иных лиц. База утечек InfoWatch насчитывает несколько тысяч зарегистрированных инцидентов.

В ходе наполнения базы каждая утечка классифицируется по ряду критериев, таких как размер организации, сфера деятельности (отрасль), размер причинённого ущерба, тип утечки (по умыслу), канал утечки, типы утекших данных, вектор воздействия.

Инциденты также классифицируются по характеру действий нарушителя. Наряду с «простыми» утечками авторы исследования выделяют следующие типы «квалифицированных» утечек:

- когда сотрудник, имеющий легитимный доступ к данным, использует данные в целях мошенничества (манипуляции с платежными данными, инсайдерской информацией);
- когда сотрудник получает доступ к данным, которые не нужны ему для исполнения служебных обязанностей (превышение прав доступа).

Исследование охватывает не более 1 % случаев предполагаемого совокупного количества утечек из-за высокого уровня латентности инцидентов, связанных с компрометацией информации. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (совокупности категорий) содержали достаточное или избыточное количество элементов — фактических случаев утечки. Такой подход к формированию поля исследования позволяет считать полученную выборку теоретической, а выводы исследования и выявленные с учетом

данной выборки тренды — репрезентативными для генеральной совокупности.

При формировании диаграмм по отдельным разрезам из выборки исключены утечки, классифицированные по основному критерию разреза как неопределенные.

Например, разрез по вектору воздействия, куда входят утечки под воздействием внешних атак и внутреннего нарушителя, не содержит утечек, для которых вектор не удалось определить. То же справедливо для распределений по виновнику, умыслу и другим критериям.

При составлении отраслевой карты и диаграмм раздела «Отраслевая карта» целенаправленно выведены за рамки исследования утечки с несоразмерно большим (более 10 млн единиц) количеством скомпрометированных персональных данных. Утечки с незначительным (менее 100 единиц) количеством утекших записей также удалены из выборки. Это сделано для того, чтобы избежать искажений, которые неизбежно вносят крупные утечки в отраслевую картину. Использование ограниченной выборки для построения диаграмм в названном разделе специально оговаривается.

Случаи нарушения конфиденциальности информации и иные инциденты информационной безопасности (ИБ), например DDoS-атаки, не повлекшие утечек данных, а также утечки с неясным источником данных, когда неизвестно, какой организации принадлежали скомпрометированные данные, не включаются в выборку.

Исследование направлено на выявление динамики процессов, характеризующих глобальную, отраслевую и региональную картину происшествий, связанных с утечками информации.

Результаты исследования

В 2016 году Аналитическим центром InfoWatch было зарегистрировано 1556 случаев утечки конфиденциальной информации (см. Рисунок 3.1). В результате утечек было скомпрометировано более 3,1 млрд записей персональных данных

(записей ПДн), — номера социального страхования, реквизиты пластиковых карт и иная критически важная информация.

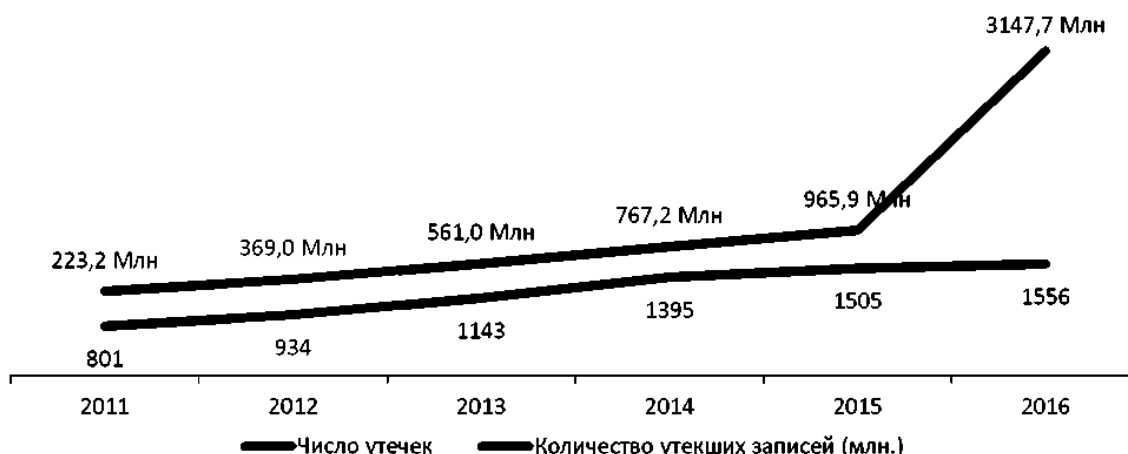


Рисунок 3.1. Число утечек информации и объем персональных данных, скомпрометированных в результате утечек. 2011 - 2016 гг.

Количественный рост утечек в 2016 году замедлился (рис. 3.2). Если в 2015 году этот показатель составил 7,9%, то в 2016 году число утечек выросло на 3,4%.

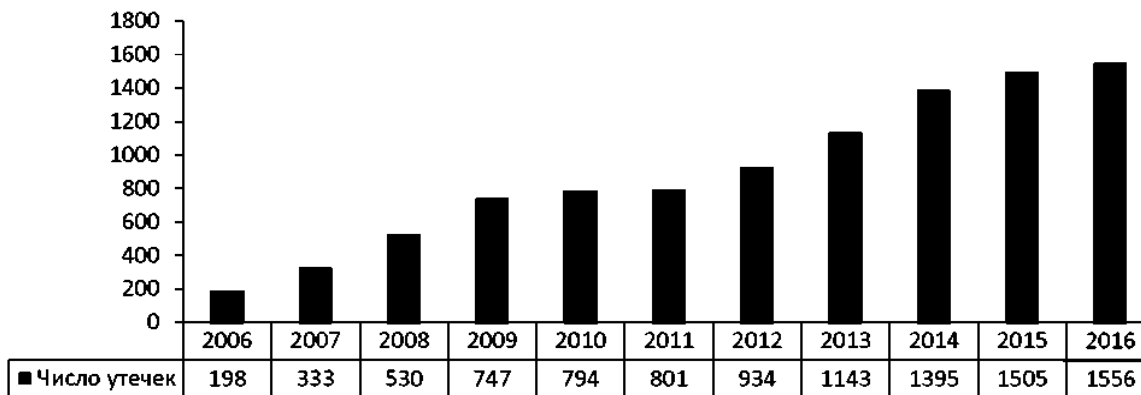


Рисунок 3.2. Число зарегистрированных утечек информации, 2006 -2016 гг.

В 2016 году впервые за все время наблюдений мы зафиксировали трехкратное увеличение объема данных, скомпрометированных в результате утечек, и столь же существенный рост числа скомпрометированных записей персональных данных в расчете на одну утечку (см. рис. 3.3). Причем увеличение объемов скомпрометированных данных не связано только с одной или несколькими крупными утечками — в

противном случае можно было бы говорить о случайном всплеске. На деле же было зафиксировано 79 утечек, в результате каждой из которых скомпрометировано более 1 млн. записей.

Таким образом, в 2016 году картина утечек претерпела существенные изменения. Мы входим в эпоху массовой компрометации данных. Основной фактор, определяющий современную картину — количественный и качественный рост утечек.

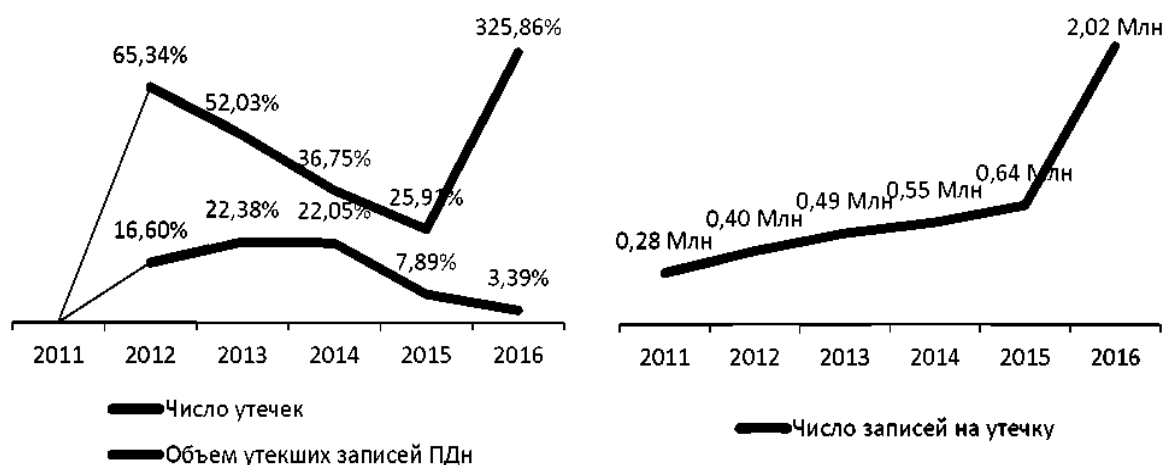


Рисунок 3.3. Динамика роста числа утечек и объема записей ПДн. Объем персональных данных, скомпрометированных в ходе одной утечки, 2011–2016 гг.

В 2016 году было зарегистрировано 540 (38,2%) утечек информации, причиной которых стал внешний злоумышленник. В 873 (61,8%) случаях - утечка информации по внутренним причинам. Доля утечек под воздействием внешних атак оказалась более чем на 6 п. п. выше аналогичного показателя 2015 года (тогда на долю утечек под воздействием внешних атак пришлось 32% утечек). В результате, в 2016 году по вине внешнего злоумышленника было скомпрометировано 2,53 млрд. записей ПДн — это составляет 80% от совокупного объема скомпрометированных за год записей. Внешние атаки спровоцировали 34 из 44 зафиксированных случаев «мега-утечек».

databreaches.net: Внешним злоумышленникам удалось украсть личную и финансовую информацию о 203 млн. клиентов Experian. Хакеры получили доступ к личной информации — именам, датам рождения, адресам, телефонным номерам и прочим данным. Дамп базы данных был выставлен на продажу, в

результате чего любой желающий мог купить эту информацию за 0,8082 биткойна (около \$640 по текущему курсу).

Утечки данных под воздействием внешних атак отличаются большим объемом компрометируемых данных. В среднем, на одну «внешнюю» утечку приходится 4,69 млн. скомпрометированных записей ПДн. Для сравнения — в результате одной утечки данных по вине или неосторожности внутреннего нарушителя было скомпрометировано в среднем 0,56 млн. записей ПДн. Атаки «извне» имеют еще одну характерную черту — злоумышленники «выносят» из атакуемого периметра все, до чего могут дотянуться.

Motherboard: Хакер взломал сервер Минюста США и украл более 200 ГБ данных, в том числе имена, фамилии, номера телефонов, адреса электронной почты 20 тыс. сотрудников ФБР и 10 тыс. сотрудников Министерства внутренней безопасности. По информации Motherboard, злоумышленнику удалось взломать аккаунт сотрудника Министерства внутренней безопасности, после чего хакер связался с оператором ФБР и, выдавая себя за легитимного пользователя, получил доступ к инфраструктуре Министерства юстиции.

Не менее интересен «информационный эффект», связанный с внешними утечками. Любая крупная утечка требует от пострадавшей организации публичной реакции. Далеко не всегда пресс-службам организаций удастся с честью решить эту задачу. Иногда утечка выступает поводом для отставки руководителей организации, государственных служащих.

Thesmokinaaun.com: Персональные данные членов палаты представителей Конгресса США от Демократической партии были похищены и размещены в глобальной сети Интернет. Ссылка на файл Excel с данными политиков появилась в Твиттере хакера с ником Gussifer 2.0, который ранее взял на себя ответственность за взлом сети Национального комитета Демократической партии. Тогда Gussifer 2.0 выложил около 20 тысяч электронных писем Национального комитета демократов на портале WikiLeaks. Утечка предположительно стала причиной заявления председателя комитета демократов Дебби Вассерман-Шульца о намерении уйти в отставку.

Впрочем, это не означает, что утечки, случившиеся в результате недозволенных действий внутреннего нарушителя,

менее разрушительны, чем утечки, произошедшие в результате внешнего воздействия. Основные отличия результатов внутреннего воздействия от внешнего заключаются в характере последствий для организации- жертвы.

Если эффект «внешней» утечки можно сравнить с ковровой бомбардировкой, то «внутренняя» утечка ближе к точечному бомбометанию — под угрозой оказывается критически важная информация, а размер потенциального финансового ущерба практически не ограничен и может достигать стоимости всего бизнеса пострадавшей компании.

bloombera.com: Британские букмекерские компании 888 Holdings Plc и Rank Group Plc отказались от поглощения William Hill — еще одного крупного участника игорного рынка — за 4,1 млрд. долларов США. Основная причина срыва переговоров — утечка данных на стороне William Hill.

В связи с особенностями природы внутренних утечек необходимо обратить внимание на проблему «привилегированных» пользователей — топ-менеджмента, системных администраторов, иных сотрудников, чьи права доступа к информации практически не ограничены, включая самих специалистов по информационной безопасности. Контролировать действия таких сотрудников чрезвычайно сложно, а последствия, к которым приводят ошибки или злонамеренная деятельность «высокопоставленных» нарушителей, по масштабу можно сравнить со стихийным бедствием.

Руководство компании HITSniffer, специализирующейся на веб-аналитике, объявило о приостановке бизнеса из-за кражи клиентских баз компании одним из бывших сотрудников.

В 2016 году в 36% случаев виновниками утечек информации были настоящие (33,9%) или бывшие (2,1%) сотрудники организаций. Более чем в 2% случаев была зафиксирована вина руководителей (топ-менеджмент, главы департаментов и отделов) и системных администраторов. Доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации, составила 6%.

Доля утечек персональных и платежных данных в распределении утечек по типу информации осталась на уровне прежних лет, составив 93% (см. рис.3.4).

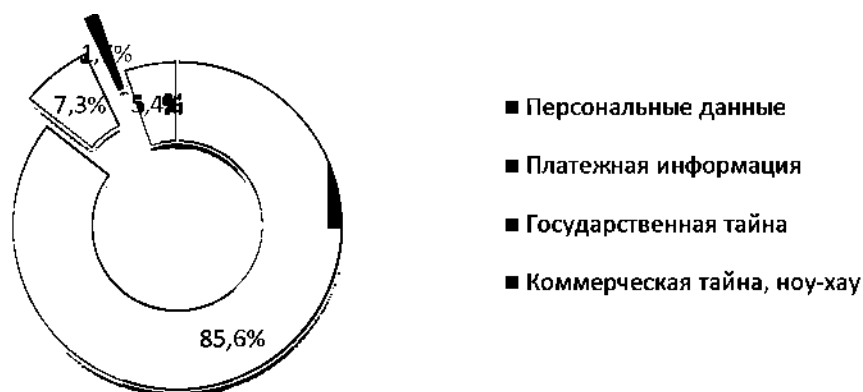


Рисунок 3.4. Распределение утечек по типам данных, 2016 г.

В 2016 году доля утечек данных, сопряженных с последующим использованием скомпрометированной информации в целях мошенничества (как правило, банковский фонд), снизилась на 3,3 п. п. до 7%.

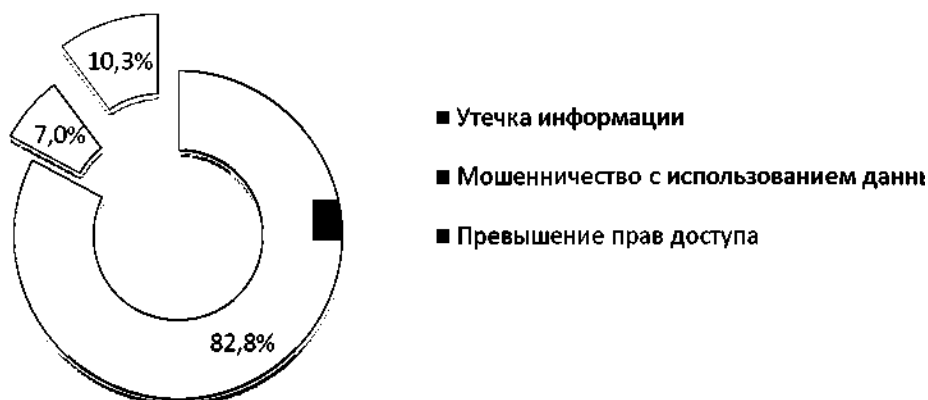


Рисунок 3.5. Распределение инцидентов по характеру, 2016 г.

10% инцидентов классифицированы как нарушения, сопряженные с получением несанкционированного доступа к информации (превышение прав доступа, манипуляция с информацией, которая не нужна сотруднику для исполнения служебных обязанностей).

Выводы

Трехкратное увеличение объема скомпрометированных данных свидетельствует о растущей день ото дня ценности

информации в цифровом виде. Причем если количественный рост утечек прогнозировать сложно — не исключено, что он попросту остановится, то сценарий, при котором объем скомпрометированных данных растет год от года, следует считать наиболее вероятным.

РИА Новости: В результате хакерской атаки на инфраструктуру французской компании DCNS, которая занимается строительством подводных лодок, похищены 22,4 тыс. страниц секретной документации. Французская госкомпания DCNS участвует в проекте по строительству шести субмарин класса Scorpene для индийского флота и одновременно строит 12 подлодок по заказу ВМФ Австралии. В результате утечки описания коммуникационных систем, подводных датчиков, систем боевого управления, навигационных систем и систем пуска торпед оказались в руках австралийского издания и, возможно, третьих лиц.

Небольшая доля умышленных утечек через мобильные устройства, съемные носители, электронную почту и бумажные документы объясняется тем, что злоумышленники все меньше используют эти каналы для совершения противоправных действий. «Продвинутый» нарушитель осведомлен, что современные средства контроля позволяют успешно перехватывать передачу конфиденциальной информации по этим каналам, и не рискует понапрасну.

Доминирование сетевого канала в распределении случайных и умышленных утечек свидетельствует, во-первых, о растущем значении этого канала для бизнеса. Число коммуникационных сервисов, «завязанных» на сеть, огромно. Количество ошибок сотрудников, работающих с этими сервисами, год от года только увеличивается. Как следствие, растет доля случайных утечек при передаче информации по сети и публикации данных в интернете.

С другой стороны, злоумышленники все реже используют заведомо контролируемые каналы передачи информации — электронную почту, сервисы мгновенных сообщений. В этом смысле сеть все еще остается каналом передачи данных, где возможности систем контроля и защиты в целом превосходят возможности злоумышленников.

Контрольные вопросы:

1. Охарактеризуйте принципы классификации уязвимостей по стандартам 2011 года и 2015 года. Дайте пояснение, в чем они солидарны и в чем различаются.
2. Дайте пояснение, в чем состоит новизна подходов к описанию уязвимостей и их классификации в новых стандартах 2015 года.
3. Поясните суть и результаты проверочных мероприятий по оценке мер защиты от КР по стандарту ГОСТ Р ИСО/МОК 27004-2011.
4. Поясните выводы анализа компании InfoWatch инцидентов безопасности в 2016 году.

Задания для самостоятельной работы к главе 3:

Вариант № 1. Какие шаги применяются для оценки рисков? Обосновать перечень.

Вариант № 2. Как производится идентификация уязвимостей системы от средств компьютерной разведки?

Вариант № 3. Приведите шаги методологии уменьшения риска, вычленив из нее риски, связанные с применением средств и методов компьютерной разведки.

Вариант № 4. Что (какие данные) должно включать в себя утверждение о результатах оценки рисков применения методов компьютерной разведки (утверждение формулируется в виде пары: угроза применения компьютерной разведки-уязвимость)?

4. Средства и методы обнаружения вторжений в информационные системы

Системами обнаружения вторжений (СОВ) называют множество различных программных и аппаратных средств, объединяемых одним общим свойством — они занимаются анализом использования вверенных им ресурсов и, в случае обнаружения каких-либо подозрительных или просто нетипичных событий, способны предпринимать некоторые самостоятельные действия по обнаружению, идентификации и устранению их причин.

Но системы обнаружения вторжений лишь один из инструментов защитного арсенала, и он не должен

рассматриваться как замена любому другому защитному механизму. Защита информации наиболее эффективна, когда в интрасети поддерживается многоуровневая защита. Она складывается из следующих компонентов:

- политика безопасности интрасети организации;
- система защиты хостов в сети;
- сетевой аудит;
- защита на основе маршрутизаторов;
- межсетевые экраны;
- системы обнаружения вторжений;
- план реагирования на выявленные атаки.

Следовательно, для полной защиты целостности сети необходима реализация всех вышеперечисленных компонентов защиты, и использование многоуровневой защиты является наиболее эффективным методом предотвращения несанкционированного использования компьютерных систем и сетевых сервисов. Таким образом, система обнаружения вторжений — это одна из компонент обеспечения безопасности сети в многоуровневой стратегии её защиты.

4.1. Выявление и отражение компьютерных атак

Для выявления и отражения в дальнейшем компьютерных атак, как средства реализации задач компьютерной разведки, необходимо, прежде всего, сформировать правильные взгляды на информационные процессы, проходящие не только в компьютерной сети, но и во всей ИС. Система обнаружения компьютерных атак, по сути, является специализированной системой обработки информации, предназначенной для чрезвычайно быстрого анализа огромного объема данных совершенно разного вида. Для того чтобы определить наиболее точно критерии эффективности такой системы и оценить параметры, которые наиболее сильно влияют на скорость и точность работы, необходимо проанализировать, какого рода данные будут обрабатываться в системе и каким образом это должно происходить.

При этом следует учитывать тот факт, что система обнаружения атак должна функционировать адекватно угрозам

безопасности, характерным для рассматриваемых объектов информационной системы, поэтому исходной позицией является выявление перечня угроз, характерных для данной ИС. К сожалению, практически все существующие системы обнаружения компьютерных атак лишены функциональности, позволяющей связывать риски и угрозы безопасности с происходящими в сетевой и локальной вычислительной среде событиями. В результате такого одностороннего анализа, когда в расчет принимаются только технические параметры сети, причем их весьма ограниченное количество, страдает в первую очередь качество обнаружения атак. Более того, пользователь такой системы никогда не получит той информации, ради которой эти системы эксплуатируются — информации о реализации угроз безопасности, которым подвержены защищаемые сетевая и локальная инфраструктуры.

Обнаружение угроз безопасности

Для описания нового подхода введем понятия, которые будут применяться в дальнейшем. Под информационной системой в данной работе будет пониматься совокупность технических средств (компьютеров, коммуникационного оборудования, линий передачи данных), при помощи которых обеспечивается обработка информации в организации.

Под угрозой информационной системе будем понимать потенциально возможное действие, предпринимаемое злоумышленником, которое может привести к прямому или косвенному ущербу. В этом предложении рассматриваются действия, направленные на нарушение установленных владельцем правил функционирования системы, выполняемые при помощи различных средств вычислительной техники.

Целью приведенной ниже концепции обнаружения угроз информационной безопасности является определение новых требований и принципов конструирования систем обнаружения компьютерных атак, ориентированных на комплексную обработку информации о защищаемой инфраструктуре для своевременного выявления и предупреждения о возможности реализации угроз, присущих информационной системе.

На сегодня пирамида информационной обработки данных в современной СОА выглядит следующим образом (рис. 4.1).



Рисунок 4.1. Информационная пирамида

Верхняя часть информационной пирамиды — это риски и угрозы, присущие рассматриваемой системе. Ниже располагаются различные варианты реализаций угроз (атаки), и самый нижний уровень — это признаки атак. Конечный пользователь, равно как и система обнаружения атак, имеет возможность регистрировать только процесс развития конкретной атаки или свершившийся факт атаки по наблюдаемым характерным признакам. Признаки атаки — то, что мы реально можем зафиксировать и обработать различными техническими средствами, а следовательно, необходимы средства фиксации признаков атак.

Если данный процесс рассматривать во времени, то можно говорить, что определенные последовательности наблюдаемых признаков порождают события безопасности. События безопасности могут переводить защищаемые объекты информационной системы в небезопасное состояние. Следовательно, для системы обнаружения атак необходим информационный срез достаточной полноты, содержащий все события безопасности, произошедшие в информационной системе за рассматриваемый период. Кроме того, поднимаясь вверх по

пирамиде, для события безопасности можно указать, к реализации какого вида угроз оно может привести, для того чтобы в процессе развития атаки производить прогнозирование ее развития и принимать меры по противодействию угрозам, которые может вызывать данная атака.

Методология обработки данных в современных информационных системах подразумевает повсеместное использование многоуровневости. Для СОА нового типа можно выделить следующие крупные уровни, на которых возможно осуществление доступа к обрабатываемой информации.

Вообще говоря, современные системы обнаружения атак еще далеки от эргономичных и эффективных с точки зрения безопасности решений. Повышение же эффективности следует ввести не только в области обнаружения злонамеренных воздействий на инфраструктуру защищаемых объектов информатизации, но и с точки зрения повседневной «боевой» эксплуатации данных средств, а также экономии вычислительных и информационных ресурсов владельца данной системы защиты.

Если же говорить непосредственно о модулях обработки данных, то, следуя логике предыдущего раздела, каждая сигнатура атаки в представленной схеме обработки информации об атаке является базовым элементом для распознавания более общих действий — распознавания фазы атаки (этапа ее реализации). Само понятие сигнатуры обобщается до некоторого решающего правила (например, с помощью поиска аномалий в сетевом трафике или клавиатурном почерке пользователя). А каждая атака наоборот разбивается на набор этапов ее проведения. Чем проще атака, тем проще ее обнаружить и больше возможностей появляется по ее анализу. Каждая сигнатура отображает определенное событие в вычислительной сетевой и локальной среде в фазовое пространство компьютерных атак. Фазы можно определить свободно, но лучше сохранять при этом достаточную степень детализации, чтобы иметь возможность описывать атаки с помощью подробных сценариев атак (списка фаз атак и переходов между ними).

Сценарий атаки в этом случае представляет собой граф переходов, аналогичный графу конечного детерминированного автомата. А фазы атак можно описать, например, следующим образом:

- опробование портов;
- идентификация программных и аппаратных средств;
- сбор баннеров;
- применение эксплойтов;
- дезорганизация функционала сети с помощью атак на отказ в обслуживании;
- управление через «бэкдоры»;
- поиск установленных троянов;
- поиск прокси-серверов;
- удаление следов присутствия и т. д. (по необходимости с различной степенью детализации).

Преимущества такого подхода очевидны — в случае раздельной обработки различных этапов атаки появляется возможность распознавать угрозу еще в процессе ее подготовки и формирования, а не на стадии ее реализации, как это происходит в существующих системах. При этом элементной базой для распознавания может быть как сигнатурный поиск, так и выявление аномалий, использование экспертных методов и систем, доверительных отношений и прочих информационных, уже известных и реализованных, сетевых и локальных примитивов оценки происходящего в вычислительной среде потока событий. Обобщающий подход к анализу позволяет соответственно определять и распределенные (во всех смыслах) угрозы как во временном, так и логическом и физическом пространствах. Общая схема обработки поступающих событий также позволяет осуществлять поиск распределенных атак — путем последующей агрегации данных из различных источников и конструирования метаданных об известных инцидентах по защищаемому «периметру» (рис. 4.2).

Разбиение атаки на более мелкие (фазы) позволяет:

- осуществлять более точное распознавание атак (чем проще атака, тем проще ее обнаружить);
- понять, каким должно быть реагирование на атаку;
- использовать классификатор угроз и прогнозировать поведение атакующего;
- комбинировать поиск атак на уровне хоста и сетевом уровне. Управление трояном. Идея достаточно проста — для управления трояном используется скрипт, написанный на PHP,

ASP, Perl или чём-нибудь подобном. Скрипт может размещаться на любом хостинге с поддержкой соответствующих сценариев.

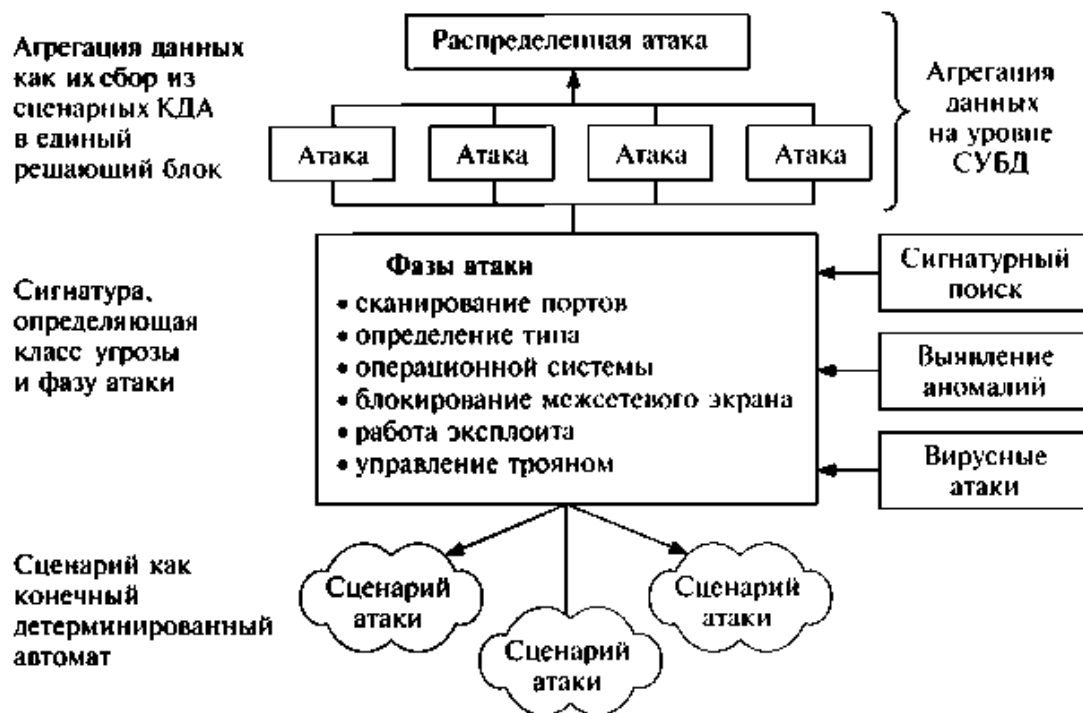


Рисунок 4.2.Схема интегрального обнаружения компьютерных атак

Обмен информацией с трояном происходит следующим образом: когда хакер хочет передать трояну команду, он по HTTP-протоколу посылает её скрипту. Скрипт принимает команду и где-то её сохраняет (например, в текстовом файле у себя на сервере), как только троян обратится к скрипту и «спросит», не было ли чего-нибудь от хакера, скрипт отдаст ему сохранённую команду. Естественно, для того чтобы вовремя узнавать о поступивших командах, трояну нужно регулярно обращаться к скрипту.

Распределенные атаки выявляются путем агрегации данных о поступающих атаках и подозрительных действиях и сопоставления шаблонов и статистической фильтрации. Таким образом, оповещение о подозрительных действиях в компьютерных системах происходит на нескольких уровнях:

- нижний уровень сообщает о примитивных событиях (совпадении сигнатур, выявлении аномалий);

- средний уровень извлекает информацию из нижнего уровня и агрегирует ее с помощью конечных автоматов (сценариев атак), статистического анализа и механизмов пороговой фильтрации;

- высший уровень агрегирует информацию с двух предыдущих и позволяет выявлять обычные и распределенные атаки, их реальный источник и прогнозировать его дальнейшее поведение на основе интеллектуального анализа.

Ядро системы обнаружения компьютерных атак должно быть четко разделено с системой визуализации и сигнализации.

4.2. «Антихакинг» как система выявления признаков злонамеренного изучения открытых сервисов и защитных механизмов системы. Правила безопасного использования Интернета и соцсетей

«Антихакинг» как система выявления признаков злонамеренного изучения открытых сервисов и защитных механизмов системы (признаки компьютерной разведки) основан на знании хакерских методов изучения систем, с одной стороны, а с другой – основан на выявлении тех из уязвимостей и брешей в защите, которые используются для КР.

Начнем с основ. Ни один компьютер не сможет работать без операционной системы. Сразу же оговоримся, что мы не будем подливать масла в огонь и рассуждать о том, что лучше — Linux, Windows или продукция Apple. Подойдем к выбору более рационально. Если в вашей сети все пользователи работают под Windows, то вполне логично, что вы тоже должны использовать ее в качестве своей основной рабочей ОС. Это позволит вам оперативно реагировать на различные проблемы и понимать то, как чувствует себя в вашей сети рядовой пользователь. Очень важно понимать, что не пользователи работают на нас, а мы работаем для пользователя. Ему всегда должно быть уютно и безопасно в наших владениях.

Если же вы администратор гетерогенной сети, то вполне логично установить первой ОС ту, в которой вы лучше разбираетесь. Это поможет сделать вашу работу комфортной, эффективной и безопасной.

Наверное, вы уже заметили, что мы говорим о первой ОС. На самом деле было бы здорово иметь под рукой тестовую машину, никак не связанную с вашей сетью и имеющую отдельный выход в Интернет. Вот тут у вас и появляется простор для творчества. Вы можете тестировать различные обновления и операционные системы, исследовать подозрительные файлы и проверять, как выглядит ваша инфраструктура извне.

Еще один пункт, который надо иметь в виду, — приватность. Весьма заманчиво, получив должность специалиста по ИБ в компании из списка Fortune 500, сразу же рассказать об этом на своей страничке в социальной сети, однако это будет плохой идеей, и из-за этого вас могут даже уволить. Обязательно уделите пристальное внимание вопросам сохранения приватности. Предъявляйте к себе более высокие требования, чем к рядовым сотрудникам.

Поскольку изолировать себя от общества нереально — мы, люди, являемся социальными существами — будет хорошей идеей завести себе виртуального двойника в сети. Создайте себе новый профиль в социальной сети, заведите еще один адрес электронной почты на одном из бесплатных сервисов. А затем уже смело используйте эти данные для регистрации на различных сайтах и тематических форумах. Главное — чтобы указываемая вами при создании «нового» человека информация никоим образом не была связана с вами. А это значит, что нельзя указывать при регистрации свой настоящий e-mail, даже если он будет использоваться только для восстановления пароля, то же самое касается номера телефона. Нельзя заходить в социальную сеть, используя новый профиль, со своего смартфона. Нельзя использовать одни и те же вопросы для восстановления пароля или же другие, но при этом указывая для ответа настоящие данные. Этот список можно продолжать очень долго — следите за собой и не ленитесь придумать по-настоящему нового человека.

Предположим, что вы создали нового человека, но что же дальше, ведь на этом все не заканчивается. Отвлечемся на мгновение от фантазий на тему «каким бы я хотел видеть свое второе я» и зададимся одним простым вопросом: когда у вас что-то не получается или вы не знаете ответа, куда вы прежде всего обращаетесь за помощью? Мы уверены, что большая часть наших

читателей ищет ответы в Google или Яндекс. Вы никогда не замечали одну особенность? Если вы, предположим, искали новую летнюю резину для своей любимой машины или более хорошую видеокарту для домашнего компьютера, то, даже если вы приобрели заветную вещь, еще очень долго самые разные сайты будут показывать вам релевантную рекламу в надежде на то, что вы сделаете эту покупку еще раз и именно у них.

Есть несколько способов избежать этого и сохранить свои предпочтения в тайне. Самый простой способ — использовать поисковые системы, не собирающие персональные данные. Подобные поисковые системы обычно работают с более крупными поисковиками, такими как Google, Yahoo!, Bing и т. д., что, в свою очередь, гарантирует качество и релевантность результатов поиска на должном уровне. Однако в отличие от крупных поисковиков они заботятся о вашей приватности, в частности они не раскрывают ваш адрес, данные о вашей системе, программном обеспечении, местонахождении и многом другом. Исходя из опыта, можно порекомендовать следующие сервисы: disconnect.me; duckduckgo.com; startpage.com.

Следующий момент, которого хотелось бы коснуться, — безопасные браузеры. Сразу же оговоримся, что мы не рекомендуем устанавливать такие браузеры всем пользователям вашей сети. ИБ всегда балансирует между максимальной защищенностью и удобством работы. А такие браузеры вызовут недовольство у рядовых сотрудников, что может привести к тому, что руководство заставит вас вернуть пользователям привычное им ПО.

Есть два основных типа браузеров — созданные с целью сохранения приватности и использующие различные надстройки для обеспечения безопасности пользователя.

В качестве примера первого типа браузера можно привести Epic privacy browser. Он был создан на основе Chromium — браузера с открытым исходным кодом, разработанного компанией Google. Его основная задача — защита вашей приватности. Все куки уничтожаются после каждой сессии, трафик проходит через серверы разработчиков, позволяя скрыть ваш IP-адрес, а соединение с веб-сайтами осуществляется преимущественно через SSL.

Примером браузера, который использует различные надстройки для обеспечения приватности, может служить Comodo dragon на основе Chromium или Comodo icedragon на основе Mozilla Firefox.

Одной из особенностей данного браузера — на наш взгляд, очень важной — является использование им своих собственных DNS-серверов. А это, в свою очередь, позволяет защититься от фишинговых атак и от возможности попадания вредоносных программ на вашу рабочую станцию.

Еще одна интересная вещь — это виртуальная среда, в которой браузер запускается в изолированном от остальной системы режиме, но, к сожалению, данная опция доступна только обладателям продукта Comodo Internet Security.

Имеются и другие браузеры, нацеленные на сохранение вашей приватности, — Brave, Dooble, Avira Scout и т. д., их мы оставляем на ваше самостоятельное рассмотрение.

В ключе разговора о браузерах мы хотели бы рассмотреть одно любопытное дополнение. К сожалению, оно недоступно для пользователей Google Chrome через магазин приложений, и скоро вы поймете почему.

Наш разговор пойдет об AdNauseam. В отличие от других расширений оно не только прячет нежелательные рекламные объявления, но еще и имитирует проходы по ним. Что приводит к тому, что собирающие о вас информацию системы начинают предполагать, что вас интересует все, начиная от похудения и заканчивая проблемами миграции кенгуру в брачный период. Естественно, что в этом огромном объеме данных ваши настоящие интересы просто затеряются.

Так почему же Google не позволяет своим пользователям устанавливать это расширение? Во-первых, это связано с тем, что эта компания является одним из лидеров по сбору и обработке персональных данных. Вторая причина — бизнес-модель. Пользователи рекламной сети Google не платят за показы рекламы, а только за переходы по объявлениям. Использование данного плагина ведет к убыткам, поскольку клик по ссылке был и деньги за него были списаны, а реального перехода не произошло. AdNauseam, как бы издеваясь над всей отраслью контекстной

рекламы, показывает примерную сумму, на которую она уже «накликала».

Раз уж зашел разговор о ПО, созданном для защиты вашей приватности, было бы огромным упущением с нашей стороны не рассказать об ОС, созданных с той же целью.

Большая часть из них представляет собой модификации Debian или Ubuntu. Операционные системы данного класса можно запускать с внешних носителей, таких как DVD. Преимущество такого подхода в том, что даже если во время работы на вашу рабочую станцию проникло вредоносное ПО, после перезагрузки вы опять получите чистую и нетронутую ОС.

К тому же такие ОС уже сконфигурированы для использования сети Tor, что безусловно помогает вам обеспечить свою приватность и даже посещать закрытые сайты.

Как правило, такие ОС не ограничиваются одним лишь использованием Tor, они поставляются с большим количеством предустановленного и настроенного ПО, в том числе для:

- шифрования и дешифровки носителей, электронной почты и другой информации;
- безопасного пользования Интернетом (про браузеры такого типа мы говорили чуть выше);
- использования генераторов и менеджеров паролей;
- обеспечения удобной и безопасной работы с сетью.

На взгляд специалиста по безопасности, среди огромного множества таких систем наибольшего внимания заслуживают:

- Tails — одна из самых бурно развивающихся. Известна тем, что эту ОС использовал Эдвард Сноуден;
- Whonix — предназначена для использования в качестве гостевой изолированной ОС, работающей в VirtualBox и использующей сеть Tor;
- IprediaOS — в отличие от других проектов вместо Tor использует I2P и построена на основе Fedora Linux;
- Discreete Linux — обеспечивает высокий уровень защиты и предназначена для людей, не имеющих глубоких знаний в области ИТ.

Безусловно, мы не рассмотрели множество прочих аспектов обеспечения индивидуальной безопасности отдельных хостов сети, но мы надеемся, что специалист по безопасности не забывает о

регулярном обновлении ПО, установке антивируса, шифровании диска, использовании шифрования и блокировки телефона, создании безопасных паролей и о многом другом, что составляет основу личной информационной безопасности.

Соблюдение правил безопасности при использовании Интернет-сервисами и соцсетями

Официально администрация США давно разместила информацию, когда и на какие средства «поддержала стартапы» по созданию международных соцсетей и сервисов, но особо не афиширует эти факты. В настоящее время более 10 комитетов при Госдепе, разведведомствах и частных фондах работают по управлению «процессами» в соцсетях, облачных и других сервисах сети Интернет. Во всех последовавших «цветных» революциях «отметились» эти комитеты и ведомства, которые потратили на свои программы массу средств на «развитие демократии» за рубежом США.

Но и криминальные злоумышленники «не спят», используют сайты социальных сетей не только для поиска компромата, но и для атаки на вас или ваши мобильные устройства.

Предлагается применять некоторые простые советы по использованию соцсетей, которые помогут вам повысить свою безопасность.

- Думайте перед тем, как сообщать информацию о себе, своих взглядах, планах и оценках, фотографиях и видеороликах. Как это можно использовать против вас?

- Логин. Используйте для защиты аккаунта только надёжный пароль и никому его не сообщайте или не используйте повторно для других сайтов. Кроме того, многие сайты поддерживают более надёжную аутентификацию, например, двухступенчатую проверку. По возможности, пользуйтесь ей. © The SANS Institute 2013 <http://www.securingthehuman.org>.

- Шифрование. Большинство сайтов социальных сетей используют сетевой протокол HTTPS для безопасного соединения. HTTPS обеспечивает шифрование данных при передаче по компьютерным сетям. Некоторые сайты, такие как Twitter, Google+ используют этот протокол по умолчанию, на других нужно

сконфигурировать соединение HTTPS. Используйте безопасный протокол HTTPS, если это возможно.

- Электронная почта. С осторожностью относитесь к письмам, которые приходят от имени социальных сетей: злоумышленники легко могут подделать их для атаки. Самый безопасный способ ответа на такие письма непосредственно с самого сайта социальных сетей, например, из закладок; проверяйте сообщения или уведомления только с Web-сайта.

- Вредоносные ссылки/Обман. Будьте осторожны с подозрительными ссылками или ложными публикациями на сайтах социальных сетей. Киберпреступники могут размещать вредоносные ссылки. Если вы «щелкните» по ним, то попадёте на вредоносные сайты, которые попытаются заразить ваш компьютер. Внимание, если пришло сообщение от друга, это не значит, что он его отправлял - его аккаунт могли взломать. Поэтому если вы получили подозрительное сообщение от члена семьи или друга (например, что его ограбили и ему нужны деньги), свяжитесь с ним по телефону, чтобы развеять сомнения.

- Приложения. Некоторые социальные сети предоставляют возможность установить программы, созданные сторонними разработчиками, например, игры. Помните, эти программы подвергаются минимальной проверке или вовсе не проверяются на предмет наличия недекларированных функций и вредного кода, через них можно получить контроль над вашим аккаунтом или доступ к персональным данным. Устанавливайте только те приложения, которые вам действительно нужны, загружайте их с известных, проверенных сайтов и сразу же удаляйте после использования.

- Советы по безопасному использованию социальных сетей:
<http://preview.tinyurl.com/b28a525>.

- Информация по безопасности Facebook:
<http://ru-ru.facebook.com/help/security> Facebook.

- Настройки безопасности:
<http://preview.tinyurl.com/a67munp>.

- Безопасность социальной сети ВКонтакте:
<http://vk.com/security>.

- Microsoft: Правила безопасности при использовании социальных сетей: <http://preview.tinyurl.com/anqnbp5>.

- Термины ИБ: <http://preview.tinyurl.com/6wkpaе5>.
- Ежедневные советы по информационной безопасности

Института SANS: <http://preview.tinyurl.com/6s2wrkp>.

Социальные сети представляют собой мощный и удобный способ общения с миром. Если вы будете следовать нашим рекомендациям, то ваше онлайн-общение станет безопасней. Вы можете ознакомиться с дополнительными правилами безопасности на сайте веб-сервиса, который вы используете. В случаях несанкционированной активности сообщайте в службу поддержки пользователей.

Основным препятствием на пути выстраивания системы современной защиты от навязывания мнений через соцсети может стать «псевдо-патриотизм» с постановкой заведомо «ложных целей», навязыванием борьбы с «мифическим врагом» и «мнимыми победами» в интересах заочно заработать политические бонусы на патриотизме, проблемах, войне и горе. В этих условиях может сложиться ситуация, когда активно обсуждаются насущные вроде проблемы, но виноваты во всем - власти, социальные группы, национальности, богачи и т.п. Типичными для такого рода «обработки» будут: присвоение права на «абсолютную» истину, безапелляционное навязывание догм и только своего «правильного» мнения, героизация борцов за «правое» дело, образ «врага» и «разчеловечивание» приверженцев «стана врага», мир делится для таких «проповедников» на тех кто с ними, а остальные - враги, выбора нет. Эти черты характерны для обработки и вовлечения в экстремистские и террористические сообщества. Будьте осторожны и бдительны при таких признаках в опосредованном общении в соцсетях.

Кроме того, современные средства массовой коммуникации - Интернет, мобильные сервисы, радио и телевизионные СМИ - используют разработанные изначально военными ведомствами Западных стран особые виды так называемых «ментальных вирусов». Новые виды их разрабатываются сейчас и далее как в коммерческих целях, так и в «боевых» геополитических, когда ставится задача манипулирования массовым мнением и поведением конкретных целевых групп.

Этому можно противостоять, и рецепт здесь один – это защита тех форм идентичности, которые исторически сложились у

народов бывшего СССР. При посещении информационных ресурсов (сервисов), через которые транслируются нереальные, виртуальные смыслы типа «все же знают, что..; всем известно авторитетное мнение, что...» противостоять этому якобы «общепринятому мнению» может только критическое отношение к любому общему, или авторитетному мнению, не подкрепленному доказательствами компетентных и не заинтересованных специалистов. Любое «задевшее» вас мнение кого бы то ни было проверяйте, перепроверяйте и при попытках склонить вас к какому либо образу мыслей, мнению никому не доверяйте на слово, без убедительных, проверенных вами доказательств. Если ваш опосредованный оппонент, собеседник, высказывает мнение, вызывающее у вас сомнение, задайте последовательно всего три вопроса ему:

- на основании каких источников собеседник так именно считает?

- где (из чего, откуда) эти источники взяли эту информацию?

- первичный источник информации - как и где ее получил, чем она подтверждается?

Обычно при попытках умышленной или неумышленной манипуляции вашим мнением общение на этих очевидных вопросах прерывается, или собеседник переходит на оскорбления. Это как раз и свидетельствует о бездоказательном навязывании нужного собеседнику мнения.

4.3. Системы обнаружения вторжений

Основным сдерживающим фактором применения всех существующих методов сетевых вторжений является их ограниченное признаковое пространство, которое включает в себя четыре группы параметров:

- 1) основные параметры отдельных ТСР-соединений: IP-адреса, порты, протоколы, количество байтов, продолжительность, количество пакетов;

- 2) параметры, основанные на контексте, например, количество SYN пакетов;

- 3) параметры, связанные со временем, т. е. различные условные комбинации параметров в последние T секунд;

4) параметры, определяющие соединения, т. е. различные условные комбинации параметров в последние N соединений.

Следует отметить, что эти параметры описывают только сетевую и транспортную части протокола. Хотя ряд алгоритмов используют дополнительные характеристики из прикладной части, но этого недостаточно для эффективного обнаружения аномалий протокола. Для проведения классификации СОВ необходимо учесть несколько факторов (рис. 4.3).



Рисунок 4.3. Характеристики систем обнаружения вторжений

Метод обнаружения описывает характеристики анализатора. Когда СОВ использует информацию о нормальном поведении контролируемой системы, она называется поведенческой. Когда СОВ работает с информацией об атаках, она называется интеллектуальной.

Поведение после обнаружения указывает на реакцию СОВ на атаки. Реакция может быть активной — СОВ предпринимает корректирующие (устраняет лазейки) или действительно активные (закрывает доступ для возможных нарушителей, делая недоступными сервисы) действия. Если СОВ только выдаёт предупреждения, её называют пассивной.

Расположение источников результата аудита подразделяет СОВ в зависимости от вида исходной информации, которую они

анализируют. Входными данными для них могут быть результаты аудита, системные регистрационные файлы или сетевые пакеты.

Частота использования отражает либо непрерывный мониторинг контролируемой системы со стороны СОВ, либо соответствующие периодическим запускам СОВ для проведения анализа.



Рисунок 4.4. Классификация систем обнаружения вторжений

Классифицировать СОВ можно по нескольким параметрам (рис. 4.4). По способам реагирования различают статические и динамические СОВ. Статические средства делают «снимки» (snapshot) среды и осуществляют их анализ, разыскивая уязвимое ПО, ошибки в конфигурациях и т. д. Статические СОВ проверяют версии работающих в системе приложений на наличие известных уязвимостей и слабых паролей, проверяют содержимое специальных файлов в директориях пользователей или проверяют конфигурацию открытых сетевых сервисов. Статические СОВ обнаруживают следы вторжения.

Динамические СОВ осуществляют мониторинг в реальном времени всех действий, происходящих в системе, просматривая файлы аудита или сетевые пакеты, передаваемые за определённый промежуток времени. Динамические СОВ реализуют анализ в реальном времени и позволяют постоянно следить за безопасностью системы.

По способу сбора информации различают сетевые и системные СОВ. Сетевые СОВ (network intrusion detection system, NIDS) контролируют пакеты в сетевом окружении и обнаруживают

попытки злоумышленника проникнуть внутрь защищаемой системы или реализовать атаку «отказ в обслуживании». Эти COB работают с сетевыми потоками данных. Типичный пример NIDS — система, которая контролирует большое число TCP-запросов на соединение (SYN) со многими портами на выбранном компьютере, обнаруживая, таким образом, что кто-то пытается осуществить сканирование TCP-портов. Сетевая COB может запускаться либо на отдельном компьютере, который контролирует свой собственный трафик, либо на выделенном компьютере, прозрачно просматривающим весь трафик в сети (концентратор, маршрутизатор). Сетевые COB контролируют много компьютеров, тогда как другие COB контролируют только один.

Среди преимуществ использования NIDS можно выделить следующие моменты:

- NIDS можно полностью скрыть в сети таким образом, что злоумышленник не будет знать о том, что за ним ведется наблюдение;
- одна система NIDS может использоваться для мониторинга трафика с большим числом потенциальных систем-целей;
- NIDS может осуществлять перехват содержимого всех пакетов, направляющихся на систему-цель.

Среди недостатков данной системы необходимо отметить следующие аспекты:

- NIDS может только выдавать сигнал тревоги, если трафик соответствует предустановленным правилам или признакам;
- NIDS может упустить нужный интересуемый трафик из-за использования широкой полосы пропускания или альтернативных маршрутов;
- NIDS не может определить, была ли атака успешной;
- NIDS не может просматривать зашифрованный трафик;
- в коммутируемых сетях (в отличие от сетей с общими носителями) требуются специальные конфигурации, без которых NIDS будет проверять не весь трафик.

COB, которые устанавливаются на хосте и обнаруживают злонамеренные действия на нём, называются хостовыми, или системными COB (Host-based intrusion detection system, HIDS). Примерами хостовых COB могут быть системы контроля целостности файлов (СКЦФ), которые проверяют системные

файлы с целью определения, когда в них были внесены изменения. Мониторы регистрационных файлов (Log-file monitors, LFM) контролируют регистрационные файлы, создаваемые сетевыми сервисами и службами. Цель обманных систем, работающих с псевдосервисами, заключается в воспроизведении хорошо известных уязвимостей для обмана злоумышленников.

Узловые COB представляют собой систему датчиков, загружаемых на различные сервера организации и управляемых центральным диспетчером. Датчики отслеживают различные типы событий (более детальное рассмотрение этих событий приводится в следующем разделе) и предпринимают определенные действия на сервере либо передают уведомления. Датчики HIDS отслеживают события, связанные с сервером, на котором они загружены. Сенсор HIDS позволяет определить, была ли атака успешной, если атака имела место на той же платформе, на которой установлен датчик.

Различные типы датчиков HIDS позволяют выполнять различные типы задач по обнаружению вторжений. Не каждый тип датчиков может использоваться в организации, и даже для различных серверов внутри одной организации могут понадобиться разные датчики. Следует заметить, что система HIDS, как правило, стоит дороже, чем сетевая система, так как в этом случае каждый сервер должен иметь лицензию на датчик (датчики дешевле для одного сервера, однако общая стоимость датчиков больше по сравнению со стоимостью использования сетевых COB).

С использованием систем HIDS связан еще один вопрос, заключающийся в возможностях процессора на сервере. Процесс анализа датчика на сервере может занимать 5... 15 % общего процессорного времени. Если датчик работает на активно используемой системе, его присутствие отрицательно скажется на производительности и, таким образом, придется приобретать более производительную систему.

Анализаторы журналов

Анализатор журнала представляет собой именно то, что отражает само название датчика. Процесс выполняется на сервере и отслеживает соответствующие файлы журналов в системе. Если встречается запись журнала, соответствующая некоторому

критерию в процессе датчика HIDS, предпринимается установленное действие.

Большая часть анализаторов журналов настроена на отслеживание записей журналов, которые могут означать событие, связанное с безопасностью системы. Администратор системы, как правило, может определить другие записи журнала, представляющие определенный интерес.

Анализаторы журналов по своей природе являются реактивными системами. Иными словами, они реагируют на событие уже после того, как оно произошло. Таким образом, журнал будет содержать сведения о том, что проникновение в систему выполнено. В большинстве случаев анализаторы журналов не способны предотвратить осуществляемую атаку на систему.

Анализаторы журналов, в частности, хорошо адаптированы для отслеживания активности авторизованных пользователей на внутренних системах. Таким образом, если в организации уделяется внимание контролю деятельности системных администраторов или других пользователей системы, можно использовать анализатор журнала для отслеживания активности и перемещения записи об этой активности в область, недостижимую для администратора или пользователя.

Датчики признаков

Датчики этого типа представляют собой наборы определенных признаков событий безопасности, сопоставляемых с входящим трафиком или записями журнала. Различие между датчиками признаков и анализаторами журналов заключается в возможности анализа входящего трафика.

Системы, основанные на сопоставлении признаков, обеспечивают возможность отслеживания атак во время их выполнения в системе, поэтому они могут выдавать дополнительные уведомления о проведении злоумышленных действий. Тем не менее атака будет успешно или безуспешно завершена перед вступлением в действие датчика HIDS, поэтому датчики этого типа считаются реактивными. Датчик признаков HIDS является полезным при отслеживании авторизованных пользователей внутри информационных систем.

Анализаторы системных вызовов

Анализаторы системных вызовов осуществляют анализ вызовов между приложениями и операционной системой для идентификации событий, связанных с безопасностью. Датчики HIDS данного типа размещают программную спайку между операционной системой и приложениями. Когда приложению требуется выполнить действие, его вызов операционной системы анализируется и сопоставляется с базой данных признаков. Эти признаки являются примерами различных типов поведения, которые являют собой атакующие действия, или объектом интереса для администратора СОВ.

Анализаторы системных вызовов отличаются от анализаторов журналов и датчиков признаков HIDS тем, что они могут предотвращать действия. Если приложение генерирует вызов, соответствующий, например, признаку атаки на переполнение буфера, датчик позволяет предотвратить этот вызов и сохранить систему в безопасности.

Анализаторы поведения приложений

Анализаторы поведения приложений аналогичны анализаторам системных вызовов в том, что они применяются в виде программной спайки между приложениями и операционной системой. В анализаторах поведения датчик проверяет вызов на предмет того, разрешено ли приложению выполнять данное действие, вместо определения соответствия вызова признакам атак. Например, веб-серверу обычно разрешается принимать сетевые соединения через порт 80, считывать файлы в веб-каталоге и передавать эти файлы по соединениям через порт 80. Если веб-сервер попытается записать или считать файлы из другого места или открыть новые сетевые соединения, датчик обнаружит несоответствующее норме поведение сервера и заблокирует действие.

При конфигурировании таких датчиков необходимо создавать список действий, разрешенных для выполнения каждым приложением. Поставщики датчиков данного типа предоставляют шаблоны для наиболее широко используемых приложений. Любые «доморощенные» приложения должны анализироваться на предмет того, какие действия им разрешается выполнять, и выполнение этой задачи должно быть программно реализовано в датчике.

Контролеры целостности файлов

Контролеры целостности файлов отслеживают изменения в файлах. Это осуществляется посредством использования криптографической контрольной суммы или цифровой подписи файла. Конечная цифровая подпись файла будет изменена, если произойдет изменение хотя бы малой части исходного файла (это могут быть атрибуты файла, такие как время и дата создания). Алгоритмы, используемые для выполнения этого процесса, разрабатывались с целью максимального снижения возможности для внесения изменений в файл с сохранением прежней подписи.

При изначальной конфигурации датчика каждый файл, подлежащий мониторингу, подвергается обработке алгоритмом для создания начальной подписи. Полученное число сохраняется в безопасном месте. Периодически для каждого файла эта подпись пересчитывается и сопоставляется с оригиналом. Если подписи совпадают, это означает, что файл не был изменен. Если соответствия нет, значит, в файл были внесены изменения.

По методам анализа СОВ делят на две группы: СОВ, которые сравнивают информацию с предустановленной базой сигнатур атак, и СОВ, контролирующие частоту событий или обнаружение статистических аномалий.

Анализ сигнатур был первым методом, примененным для обнаружения вторжений. Он базируется на простом понятии совпадения последовательности с образцом. Во входящем пакете просматривается байт за байтом и сравнивается с сигнатурой (подписью) — характерной строкой программы, указывающей на характеристику вредного трафика. Такая подпись может содержать ключевую фразу или команду, которая связана с нападением. Если совпадение найдено, объявляется тревога.

Второй метод анализа состоит в рассмотрении строго форматированных данных трафика сети, известных как протоколы. Каждый пакет сопровождается различными протоколами. Авторы СОВ, зная это, внедрили инструменты, которые разворачивают и осматривают эти протоколы согласно стандартам. Каждый протокол имеет несколько полей с ожидаемыми или нормальными значениями. Если что-нибудь нарушает эти стандарты, то вероятна злонамеренность. СОВ просматривает каждое поле всех протоколов входящих пакетов: IP, TCP, и UDP. Если имеются

нарушения протокола, например, если он содержит неожиданное значение в одном из полей, объявляется тревога.

Системы анализа сигнатуры имеют несколько важных сильных сторон. Во-первых, они очень быстры, так как полный анализ пакета — относительно тяжелая задача. Правила легко написать, понять и настроить. Кроме того, имеется просто фантастическая поддержка компьютерного сообщества в быстром производстве сигнатур для новых опасностей. Эти системы превосходят все другие при отлове хакеров на первичном этапе: простые атаки имеют привычку использовать некие предварительные действия, которые легко распознать. Наконец, анализ, основанный на сигнатуре, точно и быстро сообщает, что в системе все нормально (если это действительно так), поскольку должны произойти некие особые события для объявления тревоги.

С другой стороны, СОВ, основанная только на анализе сигнатур, имеет определенные слабости. Являясь первоначально очень быстрой, со временем скорость ее работы будет замедляться, поскольку возрастает число проверяемых сигнатур. Это существенная проблема, поскольку число проверяемых сигнатур может расти очень быстро. Фактически, каждая новая атака или действие, придуманное атакующим, увеличивает список проверяемых сигнатур. Не помогут даже эффективные методы работы с данными и пакетами: огромное количество слегка измененных атак могут проскользнуть через такую систему.

Имеется и другая сторона проблемы: так как система работает, сравнивая список имеющихся сигнатур с данными пакета, такая СОВ может выявить только уже известные атаки, сигнатуры которых имеются.

Но необходимо отметить, что согласно статистике 80 % атак происходит по давно известным сценариям. Наличие в системе обнаружения сигнатур известных атак даёт высокий процент обнаружения вторжений.

В случае анализа протоколов тоже имеются свои достоинства и недостатки. Из-за предпроцессов, требующих тщательной экспертизы протоколов, анализ протокола может быть довольно медленным. Кроме того, правила проверки для системы протокола трудно написать и понять. Можно даже сказать, что в этом случае приходится уповать на добросовестность

производителя программы, так как правила относительно сложны и трудны для самостоятельной настройки.

На первый взгляд, COB на основе анализа протокола работают медленнее, чем системы на основе сигнатуры, они более «основательны» в смысле масштабности и результатов. Кроме того, эти системы ищут «генетические нарушения» и часто могут отлавливать свежайшие «эксплоиты нулевого дня». COB можно разбить на следующие категории:

- системы обнаружения атак на сетевом уровне (Network IDS, NIDS) контролируют пакеты в сетевом окружении и обнаруживают попытки злоумышленника проникнуть внутрь защищаемой системы (или реализовать атаку типа «отказ в обслуживании»);

- системы контроля целостности (System integrity verifiers, SIV) проверяют системные файлы для того, чтобы определить, когда злоумышленник внес в них изменения;

- мониторы регистрационных файлов (Log-file monitors, LFM) контролируют регистрационные файлы, создаваемые сетевыми сервисами и службами.

Контрольные вопросы:

1. Назовите характеристики COA.
2. Назовите характеристики COB.
3. Дайте определение и охарактеризуйте понятие «антихакинг».
4. В чем заключаются правила использования соцсетей, затрудняющие КР?

Задания для самостоятельной работы к главе 4:

Вариант № 1. Перечислите и кратко охарактеризуйте технологии построения систем обнаружения атак (как метода компьютерной разведки).

Вариант № 2. Укажите сильные и слабые стороны методов обнаружения аномалий, применяемых для выявления признаков компьютерной разведки.

Вариант № 3. Перечислите и кратко охарактеризуйте методы интеллектуального анализа данных в системах обнаружения вторжений.

5. Противодействие программным закладкам

Противодействие программным закладкам строится, с одной стороны, на построении адекватной угрозам политике компьютерной безопасности, а с другой – на определенных методах сигнатурного и эвристического сканирования, мониторинга сетевых информационных потоков, адекватных антивирусных средствах и, наконец, на изолированной программной среде.

В любом случае реализовать эти методы можно только при выполнении некоторых организационных мер безопасности.

5.1. Принципы построения политики безопасности, обеспечивающей высокую защищенность от программных закладок. Методы выявления программных закладок: сигнатурное и эвристическое сканирование. Мониторинг информационных потоков, антивирусные средства, изолированная программная среда

Все имеющиеся на данный момент методы защиты компьютерных систем от программных закладок, в частности компьютерных вирусов, можно разделить на две группы:

1) методы применения штатных защитных средств компьютерной системы для построения и поддержания политики безопасности, адекватной в отношении защиты от программных закладок;

2) методы применения специализированных антивирусных средств, предназначенных для выявления, предупреждения и пресечения разрушающих воздействий на компьютерную систему со стороны программных закладок.

Политика безопасности компьютерной системы в отношении защиты от программных закладок базируется на двух основных принципах: минимизации программного обеспечения и минимизации полномочий пользователей. Рассмотрим эти принципы подробнее.

Принцип минимизации программного обеспечения состоит в том, что в операционной системе должно устанавливаться только то программное обеспечение, которое необходимо пользователям

для выполнения своих служебных обязанностей. Неиспользуемые компоненты операционной системы, в том числе и устанавливаемые по умолчанию, должны удаляться. Чем меньше объем программного обеспечения, установленного в защищаемой системе и чем меньше разнообразие этого программного обеспечения, тем меньше вероятность того, что очередная новая уязвимость затронет данную систему.

В Windows XP по умолчанию устанавливается целый ряд программных компонент, которые в дальнейшем, как правило, не используются. К ним относятся, в частности:

- Distributed Link Tracking Client — обеспечивает монтирование DFS-каталогов удаленных компьютеров на каталоги локальных дисков с файловой системой DFS (расширение NTFS);
- Secondary Logon — позволяет стартовать процесс от имени другого пользователя, введя соответствующие имя и пароль;
- Upload Manager — поддерживает дополнительные функции передачи данных по сети.

Как развитие принципа минимизации программного обеспечения можно рассматривать рекомендацию использовать нестандартное программное обеспечение, уязвимости которого изучаются хакерским сообществом не так интенсивно. Например, веб-клиент Opera менее опасен с точки зрения уязвимостей кода, чем Internet Explorer, а почтовый клиент The Bat менее опасен, чем Outlook и Outlook Express. Данный факт связан отнюдь не с низким качеством программного кода Microsoft, а с тем, что интерес потенциальных нарушителей безопасности направлен в первую очередь на поиск уязвимостей в наиболее распространенных программных продуктах. Программные средства «второго эшелона» анализируются хакерами значительно менее интенсивно.

Принцип минимизации полномочий пользователей заключается в том, что каждому пользователю должны предоставляться полномочия, минимально необходимые для выполнения служебных обязанностей. Чем выше полномочия пользователя, тем выше возможности вредоносного программного обеспечения, выполняющегося от его имени. Для успешного внедрения в защищенную операционную систему программной закладки или компьютерного вируса в большинстве случаев

необходимо, чтобы внедряемый в систему вредоносный код выполнялся от имени и с полномочиями администратора.

Отсюда следует, что чем меньше времени администратор проводит в системе, тем меньше возможностей для своего внедрения имеют программные закладки и компьютерные вирусы. В защищенной системе каждый пользователь-администратор должен иметь две учетные записи: одну для решения административных задач и вторую, с полномочиями обычного пользователя — для повседневной работы, при этом первая учетная запись должна использоваться как можно реже. Если установленное в системе антивирусное программное обеспечение не требует от пользователя административных полномочий в остальной части операционной системы, данное программное обеспечение должно быть сконфигурировано именно в таком режиме.

Всегда следует избегать выходить в Интернет под учетной записью администратора. Доступ к интернет-ресурсам может предоставляться администраторам только в случае неотложной необходимости, когда стоящую перед администратором задачу невозможно решить иными средствами. Во всех случаях, когда это возможно, администратор должен работать с интернет-ресурсами под низкопривилегированной учетной записью, не дающей больших полномочий вредоносному программному коду, который может проникнуть в защищаемую систему в рамках данного сеанса.

Если это не создаст серьезных помех в работе администратора, желательно запретить администратору доступ к файлам почтовых и веб-клиентов встроенными в операционную систему средствами разграничения доступа.

Развитием принципа минимизации полномочий пользователей является концепция изолированной программной среды. Изолированная программная среда представляет собой политику разграничения доступа, при которой права пользователя на доступ к объекту зависят от того, посредством какого субъекта пользователь открывает объект. В отличие от дискреционной модели доступа, в изолированной программной среде возможность доступа к объекту определяется не для тройки «пользователь — объект — право», а для четверки «пользователь — объект — право

— субъект». Например, в изолированной программной среде возможна ситуация, когда доступ на запись к файлам с расширением .EXE разрешен только компиляторам и запрещен другим программам. Кроме того, в изолированной программной среде список программ, которые может запускать пользователь, задается для каждого пользователя администратором и не может быть расширен самим пользователем.

Внедрение программной закладки в компьютерную систему, поддерживающую правила изолированной программной среды, осуществляется значительно сложнее, чем внедрение закладки в систему, поддерживающую только дискреционное разграничение доступа. В операционной системе, поддерживающей обычное дискреционное разграничение доступа, закладка может внедряться в любой процесс системы, выполняющийся с достаточными полномочиями, либо закладка может породить новый процесс, ранее отсутствовавший в системе. Однако в изолированной программной среде закладка вынуждена внедряться в конкретный процесс — процесс того приложения, которое имеет доступ к интересующим закладку данным. Поддержание адекватной политики безопасности в изолированной программной среде требует от администраторов защищаемой системы значительно больших усилий, чем в условиях избирательного разграничения доступа. Наконец, ни одна из распространенных современных многопользовательских операционных систем не поддерживает систему правил изолированной программной среды, а внесение соответствующих изменений в код имеющейся операционной системы весьма трудоемко.

При соблюдении в компьютерной системе адекватной политики безопасности внедрение в систему программных закладок невозможно. С другой стороны, добиться неукоснительного соблюдения адекватной политики безопасности в компьютерной системе на протяжении длительного периода времени практически невозможно. Таким образом, для предотвращения атаки защищенной компьютерной системы программными закладками необходимы дополнительные программные (или программно-аппаратные) средства защиты. Сформулируем требования к таким средствам защиты.

Прежде всего к программным средствам защиты от закладок предъявляются те же требования, что и к любым программным продуктам, а именно:

- эффективность — система защиты от программных закладок должна эффективно справляться со своими задачами, потребляя при этом минимум аппаратных ресурсов компьютера;
- надежность — система защиты от программных закладок не должна содержать грубых ошибок, которые могли бы привести к нарушению защиты;
- простота реализации — система защиты от программных закладок не должна быть устроена чрезмерно сложно;
- простота администрирования — система защиты от программных закладок не должна быть чрезмерно сложна в управлении.

Помимо перечисленных выше требований, к системам защиты от программных закладок предъявляются требования, специфичные для данного типа программного обеспечения. К этим требованиям относятся:

- сохранение эксплуатационных качеств системы — система защиты от программных закладок не должна заметно ухудшать эксплуатационные качества защищаемой системы;
- противодействие активным воздействиям программных закладок — система защиты должна быть способна противодействовать атакам закладок, направленным непосредственно на нее;
- эшелонированность — система защиты должна сохранять свои качества при выходе из строя любого элемента.

В настоящее время для борьбы с программными закладками в компьютерных системах применяют следующие методы:

- сканирование системы на предмет наличия известных программных закладок;
- контроль целостности программного обеспечения;
- контроль целостности конфигурации защищаемой системы;
- антивирусный мониторинг информационных потоков;
- создание ловушек и др.

Рассмотрим эти методы подробнее.

Сканирование системы на предмет наличия известных программных закладок.

Данный метод заключается в том, что система противодействия программным закладкам время от времени осуществляет сканирование дисковых накопителей компьютера на предмет наличия файлов, содержащих признаки наличия программных закладок (в том числе и вирусов). Чаще всего сканирование применяется для защиты от компьютерных вирусов.

При сканировании системы могут использоваться два метода: сигнатурный и эвристический.

При сигнатурном сканировании осуществляется поиск в файлах сигнатур (или масок, в терминологии Е. Касперского) — особых участков кода и данных, характерных для некоторого вируса. Например, компьютерный вирус, заражающий .COM-файлы MS-DOS по стандартной схеме, заменяет первые три байта заражаемого файла на команду безусловного перехода на тело вируса, а само тело вируса записывает конец файла. Если известна длина тела вируса и значения некоторых байтов тела вируса (например, последних), то признаками заражения файла данным вирусом являются:

- наличие в первых байтах проверяемого файла команды перехода на адрес `длина_файла — длина_тела_вируса`;
- наличие в конце проверяемого файла определенных байт.

Таким образом, сигнатура такого вируса включает в себя:

- длину тела вируса;
- некоторый участок кода вируса, достаточно длинный для того, чтобы исключить ложное срабатывание алгоритма.

В более общем случае сигнатура вируса содержит:

- участок кода или данных, специфичный для данного вируса;
- информацию о том, где в зараженном файле должен размещаться данный участок кода.

Подавляющее большинство существующих на сегодняшний день компьютерных вирусов используют более-менее стандартные алгоритмы, что позволяет антивирусным сканерам использовать для построения сигнатур всего около 100 принципиально различных схем. Базы данных, прилагаемые к антивирусным

сканерам, фактически содержат список сигнатур для всех известных сканеру вирусов, при проверке файла сканер последовательно ищет в файле все сигнатуры, присутствующие в базе данных. Выявление вирусов, использующих нестандартные способы заражения (в частности, полиморфных вирусов) производится с использованием специальных сигнатур, имеющих особый формат, уникальный для данного вируса, часто эти сигнатуры включаются в базу данных в виде фрагментов кода, выполняющих поиск данного вируса.

Если программная закладка не использует при внедрении ассоциирование с программными модулями атакованной системы, это не означает, что она не может быть выявлена сигнатурным сканированием. Сигнатурное сканирование позволяет выявлять и такие закладки, причем сигнатура в этом случае тривиальна. Известные программные закладки (Back Orifice, NetBus и т. д.) выявляются практически всеми антивирусными сканерами.

Основным недостатком сигнатурного сканирования является то, что он не позволяет защититься от ранее неизвестных вирусов и закладок, специально разработанных для атаки данной конкретной системы. Достаточно исправить всего лишь один байт в строке, используемой антивирусным сканером в качестве сигнатуры, и модифицированный вирус (или закладка) больше не будет обнаруживаться данным сканером. Именно поэтому производители антивирусных сканеров так настойчиво твердят о необходимости регулярного обновления приручающихся к сканеру баз данных.

Метод сигнатурного сканирования пригоден только для защиты от наименее квалифицированных атак, в ходе которых не производится разработка собственного программного обеспечения, а используются готовые программные закладки, которые легко можно найти в Интернете. К достоинствам сигнатурного сканирования относятся его эффективность (с учетом приведенного ограничения), простота реализации и использования. Эксплуатационные качества защищаемой системы при применении данного метода практически не страдают. С другой стороны, этот метод не позволяет организовать надежную эшелонированную защиту, способную противодействовать активным воздействиям программных закладок. Поэтому эффективность данного метода не следует преувеличивать.

При эвристическом сканировании в программных файлах производится поиск сигнатур, типичных не для конкретных образцов компьютерных вирусов и(или) программных закладок, а для вредоносного программного обеспечения вообще. Существует целый ряд приемов программирования, которые практически не используются при создании обычного программного обеспечения, но активно применяются при разработке компьютерных вирусов и программных закладок. В ходе эвристического сканирования антивирусный сканер ищет в проверяемом файле следы применения программистом (или вирусописателем) этих приемов.

К основным признакам наличия внутри объекта компьютерного вируса или программной закладки относятся, в частности для исполняемого файла Windows:

- наличие дополнительной секции кода в конце файла;
- установленный атрибут Executable у секции, не являющейся секцией кода;
- точка входа указывает внутрь секции, не являющейся секцией кода;
- точка входа указывает на команду перехода, ведущую за пределы секции кода;
- для документа Microsoft Office — наличие в списке макрокоманд большого макроса, автоматически вызываемого при открытии, сохранении или распечатывании документа и не связанного ни с одной клавишей;
- для письма электронной почты в формате HTML:
 - наличие в теле письма большого скрипта;
 - наличие среди файлов, прилагаемых к письму, исполняемого файла или документа Microsoft Office, имеющего признаки наличия компьютерного вируса или программной закладки;
 - наличие среди файлов, прилагаемых к письму, исполняемого файла, замаскированного под файл данных (двойное расширение, очень длинное имя и т.п.);
 - наличие в теле письма внешней ссылки, указывающей на скрипт, размещенный на некотором интернет-сервере, с использованием небезопасного коммуникационного протокола;
 - для любого бинарного программного файла:

- наличие в области данных текстовых строк вида “*.EXE” и т.п.;
- наличие в области кода последовательности байт E8 00 00 00 00. Этими байтами кодируется машинная команда call <следующая_команда>, используемая вирусами и программными закладками, использующими ассоциирование, чтобы определить базовый адрес загрузки данной копии в оперативную память (чтобы «осмотреться на новом месте»);
- динамическое изменение выполняющегося кода (полиморфные преобразования).

Перечисленные признаки очень часто встречаются в объектах, с которыми произведено ассоциирование компьютерного вируса или программной закладки, но довольно редко наблюдаются при отсутствии в системе вредоносного программного обеспечения. При осуществлении эвристического сканирования антивирусный сканер ищет в каждом программном файле подобные признаки и, в зависимости от результатов поиска, делает вывод о наличии или отсутствии в исследуемом объекте компьютерного вируса или программной закладки.

Основным достоинством эвристического сканирования является то, что оно позволяет выявлять компьютерные вирусы и программные закладки, неизвестные на момент создания сканера. С другой стороны, при эвристическом сканировании часто бывают ошибки как первого, так и второго рода. Многочисленные ложные тревоги заметно подрывают доверие пользователей к эвристическому сканированию.

Существует целый ряд приемов программирования, позволяющих «обманывать» эвристические сканеры, заставляя их «не замечать» код программной закладки. Перечислим только некоторые из них.

1. Хранить строки-константы в преобразованном виде, например, вместо строки EXE”, хранить строку “ (/FYF”, а перед использованием вычесть единицу из каждого символа преобразуемой строки.

2. Вместо переключения точки входа заражаемого файла на точку входа вируса заменять одну из первых машинных команд заражаемого файла на команду перехода на точку входа вируса.

3. Вместо команды безусловного перехода `jmp <адрес_перехода>` использовать ее синонимы, например:

- `push <адрес_перехода> ret`

или

- `хог еах,еах`

`je <адрес_перехода>`

4. Использовать динамически генерируемые адреса переходов, затрудняющие анализ машинного кода сканером.

5. Использовать нестандартные способы передачи управления из функции в функцию, например, через интерфейс программных прерываний в MS-DOS или через интерфейс оконных сообщений в Windows.

К счастью, подавляющее большинство современных компьютерных вирусов и программных закладок либо вообще не применяют перечисленные методы, либо применяют их крайне примитивно. Благодаря этому вероятность ошибки первого рода (пропуск цели) для современных эвристических сканеров весьма мала.

Антивирусное сканирование может осуществляться либо путем тотального сканирования дисков компьютера через определенные промежутки времени, либо «на лету» — перед запуском каждого исполняемого файла проверяется отсутствие в нем вирусов и закладок. Каждый из этих способов имеет свои недостатки.

Основным недостатком первого способа является то, что полное сканирование современного жесткого диска может занимать десятки минут или даже часы. Поэтому тотальное сканирование не может выполняться слишком часто — это вызывает слишком большие потери времени. При практическом применении данного метода сканирования дисков редко производятся чаще, чем 1 — 2 раза в месяц, что позволяет программной закладке, проникшей в систему, осуществлять несанкционированный доступ в течение всего этого времени.

С другой стороны, сканирование файлов «на лету» приводит к ощутимому замедлению работы операционной системы. Особенно велико это замедление при загрузке больших программных модулей в тех операционных системах, в которых загрузка исполняемых файлов происходит путем отображения на

виртуальную память (к этому классу операционных систем относится и Windows). Если перед загрузкой программного модуля осуществляется его сканирование, весь исполняемый файл должен быть загружен в оперативную память, что сводит на нет все преимущества механизма загрузки исполняемых файлов посредством отображения на виртуальную память, и может приводить к снижению производительности операционной системы в несколько раз.

Подытоживая, можно утверждать, что антивирусное сканирование является весьма действенным методом противодействия вредоносным воздействиям компьютерных вирусов и программных закладок. Однако при планировании политики антивирусного сканирования следует учитывать, как перечисленные выше факторы, ограничивающие эффективность данного метода, так и неизбежное ухудшение эксплуатационных качеств защищаемой системы при применении данного метода.

Антивирусное сканирование обязательно должно применяться ко всем вирусоопасным объектам, импортируемых в защищаемую систему из недоверяемых источников. Что касается проверки объектов, уже имеющих в системе, то в большинстве случаев такая проверка целесообразна только на серверах рабочей сети, имеющих критически важное значение для обеспечения информационной безопасности всей сети. «Параноическое» применение данного метода на всех компьютерах защищаемой сети, включая обычные рабочие станции, обычно малоэффективно, поскольку в этом случае недостатки метода, как правило, перевешивают его достоинства.

5.2. Контроль целостности программного обеспечения.

Контроль целостности конфигурации защищаемой системы

Данный метод заключается в том, что для каждого программного модуля, присутствующего в защищаемой системе, заранее подсчитываются длина и контрольная сумма. Эта информация хранится в файле, зашифрованном имитостойким шифром и подписанном цифровой подписью. Время от времени осуществляется проверка программных модулей защищаемой системы на соответствие длин и контрольных сумм эталонам,

хранящимся в этом файле. Если в систему внедрена программная закладка, нарушающая целостность программного обеспечения, при очередной проверке будет обнаружено несовпадение длины или контрольной суммы программного модуля, целостность которого нарушена закладкой и хранящегося в системе эталона.

Проверка целостности программного обеспечения может производиться либо путем тотального сканирования дисков компьютера, либо может быть построена так, что целостность каждого программного модуля проверяется непосредственно перед его загрузкой. Каждый из этих способов имеет свои недостатки.

В первом случае, если жесткий диск компьютера достаточно велик, его тотальное сканирование может занимать неприемлемо долгое время. Учитывая, что установка нового программного обеспечения и переконфигурирование (в том числе и обновление версии) старого обычно происходит достаточно часто, полное сканирование компьютера должно производиться не реже, чем каждые несколько дней. В противном случае нарушения целостности, вызванные внедрением в систему программной закладки, будет трудно отличить от нарушений целостности, вызванных легальным обновлением установленных приложений. Исходя из этого, данный способ организации контроля целостности программного обеспечения часто оказывается малоэффективным — либо контроль целостности отнимает слишком много ресурсов защищаемой системы, либо администратору трудно разобраться в том, какие нарушения целостности являются несанкционированными.

Во втором случае загрузка каждого программного модуля существенно замедляется, что обусловлено тем фактом, что для осуществления контроля целостности весь проверяемый файл должен быть считан в оперативную память, в то время как при обычной загрузке с диска считываются только те фрагменты файла, которые содержат код и данные, используемые в данный момент. В результате контроля целостности кода программного обеспечения «на лету» работа операционной системы может замедляться в десятки раз. Это замедление особенно заметно в Windows-подобных операционных системах, где значительная часть системного кода выделена в динамические библиотеки,

загружаемые в адресные пространства всех процессов, как прикладных, так и системных.

В любом случае организация в системе контроля целостности программного обеспечения требует от администраторов операционной системы повышенного внимания при установке и обновлении установленных в системе приложений. Обязательно нужно иметь в виду, что программная закладка может быть внедрена в систему в момент установки или обновления программного обеспечения, когда контроль целостности бесполезен — если для исполняемого файла контрольная сумма еще не подсчитана, нарушение целостности этого файла не может быть выявлено.

Следует также иметь в виду, что программная закладка, внедренная в защищаемую систему, может вмешиваться в функционирование системы контроля целостности и навязывать ей ложную информацию. Могут быть использованы следующие методы навязывания ложной информации:

- несанкционированная модификация файла, содержащего эталоны длин и контрольных сумм исполняемых файлов;
- сохранение эталонной копии измененного исполняемого файла и «подсовывание» ее системе контроля целостности.

Контроль целостности конфигурации защищаемой системы

Данный метод заключается в том, что для всех элементов конфигурации защищаемой системы, которые могут быть изменены при внедрении в систему программной закладки, создаются эталонные копии.

В дальнейшем регулярно производится сравнение этих элементов конфигурации с их эталонными копиями. В случае несовпадения проводится детальное изучение зафиксированных изменений на предмет того, произошло ли данное изменение в результате легальных действий администраторов или в результате внедрения в систему программной закладки.

При организации проверки целостности конфигурации защищаемой системы основная проблема состоит в том, чтобы точно выделить элементы конфигурации системы, несанкционированное изменение которых может привести к внедрению программных закладок. Если не для всех таких

элементов контролируется целостность, факт внедрения программной закладки в защищаемую систему может остаться не замеченным для администраторов. Если же множество элементов конфигурации защищаемой системы, целостность которых контролируется, выбрано слишком большим, при анализе результатов проверки целостности будет зафиксировано слишком много изменений и администраторам будет трудно выбрать из них те, которые действительно могут сигнализировать о возможности внедрения в систему программной закладки.

Проверка целостности конфигурации может производиться либо путем регулярного тотального сканирования элементов конфигурации, либо при каждом обращении программы к контролируемому элементу конфигурации. Во многих операционных системах такая проверка может быть организована с использованием стандартных средств аудита.

Затраты ресурсов компьютера при контроле целостности конфигурации системы значительно меньше аналогичных затрат при контроле целостности программного обеспечения. Это обусловлено тем, что суммарный объем элементов конфигурации системы обычно значительно меньше суммарного объема имеющихся в системе исполняемых файлов.

Так же как и в случае контроля целостности программного обеспечения, программная закладка, внедренная в защищаемую систему, может навязывать ложную информацию системе контроля целостности конфигурации.

Ключи реестра ОС Windows могут использоваться программными закладками для реализации хотя бы одной из следующих задач:

- первоначальное внедрение в операционную систему путем «подсовывания» исполняемого кода под видом «неопасного» файла;
- «подсовывание» исполняемого кода программной закладки администратору операционной системы в целях несанкционированного повышения полномочий ранее внедренной закладки;
- организация автоматического запуска программной закладки при каждой новой загрузке операционной системы либо при наступлении некоторого регулярного события.

Нетрудно видеть, что для того чтобы контроль целостности конфигурации операционной системы был эффективен, подсистема контроля целостности должна фиксировать изменения большого количества разных объектов, некоторые из которых регулярно изменяются и при отсутствии в системе программных закладок. Это является одной из основных проблем при построении адекватной политики контроля целостности конфигурации защищаемой системы.

Другая серьезная проблема, возникающая при организации контроля целостности конфигурации, состоит в том, что установка в системе дополнительного программного обеспечения создает в конфигурации системе новые записи, которые также могут быть использованы программными закладками. Это еще более усложняет и без того непростую задачу точного выделения всех потенциально опасных элементов конфигурации, целостность которых необходимо контролировать.

Антивирусный мониторинг информационных потоков

Любая программная закладка так или иначе вмешивается в информационные потоки, протекающие внутри компьютерной системы, в которую она внедрена. Это вмешательство может быть обнаружено с помощью мониторинга информационных потоков. Наиболее эффективен мониторинг тех информационных потоков, которые наиболее часто связаны с программными закладками, а именно:

- информационные потоки, связанные с паролями пользователей;
- информационные потоки, связанные с обращениями к файловым системам;
- информационные потоки, связанные с обращениями к сетевым ресурсам.

Очевидно, что при организации мониторинга информационных потоков целесообразно ограничиться мониторингом только тех потоков, которые присутствуют при наличии в защищаемой системе программной закладки и отсутствуют в противном случае (или наоборот).

Например, программа аутентификации пользователя (login в UNIX или Winlogon в Windows) работает только с файлами, содержащими эталоны паролей пользователей и настройки

конфигурации самой программы. Если зафиксировано обращение такой программы к какому-то другому файлу, это может означать, что в системе присутствует перехватчик паролей.

Данный метод выявления программных закладок, помимо достоинств, имеет два очень серьезных недостатка:

1) присутствие в системе монитора, предназначенного для выявления программных закладок, может маскировать присутствие мониторов-закладок;

2) монитор, предназначенный для выявления программных закладок, сам может быть использован в качестве закладки.

5.3. Программные ловушки

Данный метод заключается в создании в защищаемой системе «заманчивых» для нарушителей объектов, доступ к которым невозможен без использования программных закладок. Все успешные обращения к таким объектам регистрируются. Например, в Windows в роли ловушки может выступать объект с атрибутами защиты Everyone — No Access, к которому регистрируются все успешные обращения пользователей. Без применения программной закладки или специальных привилегий администратора операционной системы открыть такой объект невозможно.

5.4. Организационные и административные меры защиты от программных закладок

Одной из важнейших составных частей системы защиты от программных закладок является комплекс организационных, административных и иных мер по ее сопровождению. Ни одно программное или программно-аппаратное средство защиты либо комплекс таких средств не способен обеспечить приемлемый уровень защищенности от компьютерных вирусов и программных закладок, если работа системы защиты не будет сопровождаться адекватными действиями администраторов безопасности и иных лиц, ответственных за эффективное функционирование антивирусной защиты локальной вычислительной сети.

К основным мероприятиям по организационному сопровождению антивирусной защиты сети относятся:

- инструктирование пользователей;
- просмотр и анализ данных регистрации и мониторинга;
- контроль качества аутентификационных данных пользователей защищаемой сети;
- регулярные проверки адекватности поведения лиц, ответственных за обеспечение антивирусной защиты, в случае успешных вирусных атак;
- регулярные инспекции состояния антивирусной защиты.

Рассмотрим эти мероприятия подробнее.

Инструктирование пользователей

Пользователи защищаемой сети должны быть проинструктированы:

- о необходимости хранения в тайне своих аутентификационных данных. Если аутентификационные данные представляют собой пароль условно-постоянного действия, пользователь не должен ни при каких обстоятельствах записывать его на бумагу или другие носители информации. Если аутентификационные данные представляют собой псевдослучайный ключ, хранящийся на электронном носителе информации, пользователь не должен оставлять этот носитель информации без присмотра, а также самостоятельно создавать его резервные копии без явного разрешения администратора безопасности. Категорически запрещается передавать свои аутентификационные данные для использования другими лицами;
- необходимости экстренной смены аутентификационных данных в случае их компрометации;
- принятых в сети правилах изменения аутентификационных данных;
- недопустимости попыток обхода системных политик, связанных с аутентификацией пользователя (возвращение к старому паролю путем двукратной смены пароля и т. п.);
- недопустимости нарушения правил разграничения доступа, принятых в данной сети, в том числе и из простого любопытства;
- недопустимости компьютерных игр на рабочем месте;

- недопустимости самостоятельной установки в защищаемую сеть любого программного обеспечения без явного разрешения администратора безопасности;

- недопустимости любых попыток обхода правил экспорта (импорта) информации в (из) глобальных вычислительных сетей общего пользователя, в том числе и по уважительным (с точки зрения пользователя) причинам.

Пользователи должны знать о том, что любые их действия в защищаемой сети могут быть зарегистрированы подсистемой аудита и мониторинга. Детали реализации аудита и мониторинга, в особенности действующая политика аудита и мониторинга, должны быть скрыты от пользователей. Инструктаж о правилах безопасной эксплуатации сети должен проводиться с каждым пользователем:

- при первоначальной регистрации пользователя в защищаемой сети;

- при внесении администрацией сети существенных изменений в правила безопасности;

- через регулярные промежутки времени.

Проведенные с пользователями инструктажи должны регистрироваться в специальной книге. Проинструктированные пользователи должны расписываться в соответствующей графе данной книги.

Просмотр и анализ данных регистрации и мониторинга

Данная операция должна производиться постоянно, не реже одного- двух раз в неделю, а на компьютерах-серверах — не реже одного-двух

раз в день. Эти действия могут осуществляться только пользователем- аудитором, наделенным специальными полномочиями.

Если скорость накопления данных регистрации слишком велика для того, чтобы аудитор мог просматривать накопленные данные в реальном времени, подсистема аудита и мониторинга должна предусматривать механизм запросов, позволяющий аудитору быстро получать подробную информацию о наиболее важных событиях.

Для предотвращения переполнения журналов регистрации, а также для предотвращения снижения производительности данной

подсистемы журналы регистрации должны регулярно очищаться, при этом накопленные данные должны сохраняться на внешних носителях информации. Эти носители должны подлежать строгому учету и контролю.

Контроль качества аутентификационных данных пользователей

Наиболее уязвимым звеном системы аутентификации, использующей в качестве аутентификационной информации пароли, являются «слабые» пароли, не обладающие достаточной устойчивостью к подбору нарушителем. К «слабым» паролям относятся:

- пароли недостаточной длины;
- легкоугадываемые пароли;
- пароли, представляющие собой осмысленное слово или комбинацию слов;
- пароли, имеющие ограниченный алфавит (только буквы в одном регистре, только цифры и т.п.);
- пароли, имеющие статистику естественного языка.

Значительная часть мер по повышению устойчивости парольной аутентификации реализуется с помощью программных и (или) программно-аппаратных средств, встроенных в операционные системы, функционирующие в составе защищаемой сети. Однако для обеспечения должной защиты аутентификационной информации пользователей защищаемой сети от несанкционированного доступа также необходимы следующие организационно-административные меры:

- инструктирование пользователей о необходимости использования стойких паролей, устойчивых к подбору и угадыванию;
- регулярные проверки качества паролей пользователей сети путем пробного подбора, при этом учетные записи пользователей, чьи пароли были успешно подобраны, должны немедленно блокироваться, разблокирование такой учетной записи возможно только после смены нестойкого пароля.

Регулярные проверки адекватности поведения лиц, ответственных за обеспечение антивирусной защиты сети.

В случае успешных вирусных атак лица, ответственные за обеспечение антивирусной защиты сети, должны быть готовы к

блокированию и ликвидации компьютерных вирусов и программных закладок, преодолевших функционирующую в локальной сети систему антивирусной защиты. Для обеспечения адекватной реакции персонала на успешное внедрение вируса или закладки в защищаемую сеть должны регулярно проводиться учения, в ходе которых должна детально отрабатываться процедура отражения вирусной атаки, при этом должны отрабатываться возможные нештатные ситуации.

Регулярные инспекции состояния антивирусной защиты

В ходе эксплуатации локальных вычислительных сетей, оснащенных средствами антивирусной защиты, должны регулярно проводиться инспекции (комплексные проверки) состояния антивирусной защиты сети. Целями этих инспекций являются:

- общая оценка состояния антивирусной защиты сети;
- контроль выполнения лицами, ответственными за обеспечение антивирусной защиты, требований и правил, отраженных в соответствующих должностных инструкциях;
- уточнение порядка эксплуатации и сопровождения системы антивирусной защиты с учетом специфики ее эксплуатации в данной конкретной сети, а также опыта, накопленного в ходе ее эксплуатации.

Инспекция может проводиться с привлечением как специалистов той же организации, в которой эксплуатируется защищаемая сеть, так и приглашенных экспертов. В последнем случае должны быть особо проработаны вопросы недопущения доступа inspectирующих лиц к конфиденциальной информации, лежащей за пределами их допуска.

Инспекция антивирусной защиты может осуществляться с использованием программных или программно-технических средств.

В ходе инспекции особое внимание должно уделяться следующим ее аспектам:

- наличие и корректность функционирования средств автоматического контроля версий и пакетов обновлений системы антивирусной защиты;
- наличие и корректность функционирования средств контроля целостности системы антивирусной защиты;

- наличие и корректность функционирования средств обнаружения ошибок и уязвимостей в системе антивирусной защиты;

- отсутствие искажений дистрибутива или пакетов обновления системы антивирусной защиты в процессе поставки от разработчика.

Даже самая мощная антивирусная защита не гарантирует абсолютной защищенности от компьютерных вирусов и программных закладок. Любая антивирусная защита может быть преодолена при определенном стечении обстоятельств.

Успех вирусной атаки может быть обусловлен одной из двух причин:

- ранее неизвестные и неучтенные при планировании стратегии и тактики антивирусной защиты ошибки программного либо аппаратного обеспечения системы антивирусной защиты или используемых ей компонент системного программного обеспечения защищаемой сети;

- случайное или преднамеренное нарушение требований по защите от компьютерных вирусов и программных закладок лицами, ответственными за обеспечение антивирусной защиты сети. Среди всех случаев успешных вирусных атак заметное место занимают случаи, обусловленные ошибками обслуживающего персонала защищаемой сети. Для минимизации вероятности подобных ошибок персонал сети, ответственный за обеспечение антивирусной защиты, должен обладать необходимой квалификацией.

Лица, ответственные за антивирусную защиту сети, должны иметь доступ к актуальной информации:

- о известных атаках с использованием программных закладок (в том числе и компьютерных вирусов);

- типовых проявлениях вирусных атак;

- средствах и методах предотвращения и блокирования вирусных атак;

- особенностях функционирования вирусов и закладок, а также средств противодействия им в различных программно-аппаратных конфигурациях компьютеров и сетей.

Для лиц, ответственных за обеспечение антивирусной защиты, обязательно должны быть предусмотрены те или иные формы повышения квалификации по соответствующему профилю.

В случае обнаружения факта успешного внедрения в защищаемую сеть одного или нескольких компьютерных вирусов и (или) программных закладок должны быть незамедлительно выполнены следующие мероприятия.

1. Немедленное физическое отключение защищаемой сети от глобальных вычислительных сетей общего пользования (если такое подключение имеется). Обратное подключение может быть произведено только после выполнения всего комплекса мероприятий по ликвидации последствий вирусной атаки.

2. Немедленная физическая изоляция пораженного фрагмента сети от незараженных фрагментов (если компьютерный вирус, проникший в сеть, на момент обнаружения еще не успел заразить большую часть компьютеров защищаемой сети). Обратное подключение может быть произведено только после выполнения всего комплекса мероприятий по ликвидации последствий вирусной атаки.

3. Немедленная установка всех доступных пакетов обновления как для системы антивирусной защиты, так и для всего остального программного обеспечения, функционирующего в защищаемой сети. Должны использоваться только лицензионные пакеты обновления, полученные из доверенных источников.

4. Экстренная внеплановая проверка целостности системы антивирусной защиты. В случае обнаружения нарушений целостности должно быть проведено восстановление системы антивирусной защиты из второй копии.

5. Экстренная внеплановая проверка всех компьютеров защищаемой сети на предмет наличия компьютерных вирусов и (или) программных закладок с одновременным блокированием и (или) уничтожением обнаруженного вредоносного кода. В ходе антивирусного сканирования должны использоваться базы сигнатур, полученные из лицензионных источников. Получение баз сигнатур должно производиться непосредственно перед проверкой, что гарантирует, что в ходе проверки используются новейшие версии антивирусных баз. Если в ходе проверки определенного компьютера на нем были обнаружены зараженные

объекты, то по окончании проверки должна быть проведена повторная проверка. Компьютер признается очищенным от вредоносного программного кода только после того, как проведенное сканирование показало полное отсутствие зараженных объектов на данном компьютере. В ходе антивирусного сканирования дисков проверяемый компьютер должен быть отключен от сети, за исключением случаев, когда точно известно, что вредоносный код, проникший в сеть, не имеет функций сетевого размножения.

6. Экстренная внеплановая комплексная проверка корректности функционирования системы антивирусной защиты. В случае обнаружения некорректного функционирования антивирусной защиты должны быть проведены необходимые восстановительные работы, после чего мероприятия по ликвидации вирусной атаки должны быть повторены.

7. Экстренная смена аутентификационной информации всех пользователей сети.

8. Временное изменение настроек подсистемы аудита и мониторинга в сторону увеличения числа регистрируемых событий.

9. Проверка списка субъектов доступа на предмет возможного несанкционированного создания новых субъектов доступа проникшим в сеть вредоносным кодом, а также несанкционированного назначения новых полномочий и ролей ранее зарегистрированным в сети субъектам.

10. Анализ политики аутентификации системы антивирусной защиты, а также общей политики аутентификации, принятой в сети, на предмет пересмотра в сторону усиления требований.

11. Детальный анализ политики разграничения доступа сети, включая настройки межсетевых экранов, на предмет ошибок и слабостей, которые могли сделать возможной зафиксированную атаку.

12. Перенастройка всех программных ловушек.

Контрольные вопросы:

1. Назовите принципы построения политики безопасности, обеспечивающей высокую защищенность от программных

закладок.

2. Дайте пояснение, в чем состоят методы выявления программных закладок.

3. Охарактеризуйте положительные стороны и недостатки сигнатурного и эвристического сканирования.

4. Поясните суть и ограничения контроля целостности программного обеспечения.

5. Поясните суть и ограничения контроля целостности конфигурации защищаемой системы.

6. В чем состоят преимущества и ограничения изолированной программной среды?

7. Назовите основные организационные меры защиты от программных закладок.

Задания для самостоятельной работы к главе 5:

Вариант № 1. Укажите, как формально определяется модель компьютерной разведки «наблюдатель» и какие у нее имеются типичные недостатки?

Вариант № 2. Укажите, как формально определяются модели компьютерной разведки «перехват», «уборка мусора» и «мониторы файловых систем». В чем их суть и признаки использования?

Вариант № 3. В чем сильные и слабые стороны сигнатурного и эвристического сканирования как метода противодействия программным закладкам?

Вариант № 4. Какие сильные и слабые стороны имеет метод выявления программных закладок «сканирование на лету»?

Вариант № 5. Какие сильные и слабые стороны имеет метод выявления программных закладок «контроль целостности конфигурации системы»?

6. Комплекс мер технического противодействия компьютерной разведке

Комплекс мер технического противодействия методам КР строится не хаотично – как заблагорассудится администраторам безопасности и системным администраторам защищаемых объектов. В госструктурах он строго подчинен требованиям стандартов Росстандарта и руководящих документов ФСБ России и

ФСТЭК России. В коммерческих организациях и структурах также ориентируются на российские международные стандарты, только в отличие от госструктур речь идет не о выполнении жестких требованиях защиты, а учете и управлении рисками. В любом из этих случаев речь будет идти о системе управления информационной безопасностью (далее - СУИБ).

6.1. Разработка вариантов совершенствования имеющихся мер технического противодействия компьютерной разведке на российских объектах информатизации

Залогом эффективного функционирования СУИБ является хорошо продуманная Политика СУИБ. Это тот документ, на основе которого формулируются директивы, стандарты, процедуры, руководства и другая сопутствующая документация в области ОИБ. Поэтому определив область действия, организация должна установить понятную и краткую Политику СУИБ. Имея и применяя такую политику, организация берет под контроль направления своего развития и его результаты.

Чтобы не было дальнейшей путаницы в понятиях, особо отметим, что Политика СУИБ рассматривается как надмножество (расширенное множество) ПолИБ организации, хотя эти две политики могут быть описаны в одном документе. Небольшим организациям может быть достаточно одной политики; организациям большего размера могут понадобиться различные политики. Если необходимо создание дополнительных политик (подполитик), то они должны быть определены на стадии, когда начинается разработка основной Политики СУИБ.

Политика СУИБ — документ верхнего уровня, заявляющий о целях организации, намерениях, задачах и средствах достижения целей в определённой области действия СУИБ. Ее цель - обеспечение управления и поддержки ИБ со стороны руководства организации, поскольку для эффективного управления рисками ИБ требуется привлечение значительных ресурсов. Политика СУИБ предназначена для создания программы ОИБ (она предусматривает разработку и поддержку детальных процессов и процедур ОИБ в масштабе организации, совместимых с политикой), установления

целей и задач функционирования СУИБ и распределения ответственности в рамках области действия СУИБ.

Таким образом, Политика СУИБ должна:

- соответствовать идентифицированной области действия СУИБ;
- включать в себя основные положения для определения целей;
- устанавливать цели функционирования СУИБ, основанные на требованиях и приоритетах в отношении ИБ организации;
- определять общие направления и принципы деятельности по отношению к ИБ, которые должны быть достигнуты при использовании СУИБ;
- учитывать бизнес-требования, а также требования нормативно-правовой базы и договорных обязательств;
- учитывать риск-ориентированный подход, принятый в организации, вводить критерии оценки рисков ИБ и определять структуру оценки рисков ИБ (например, в соответствии с ГОСТ Р ИСО/МЭК 27005- 2010 и ISO/IEC 27005:2008);
- устанавливать ответственность высшего руководства организации, связанную с СУИБ;
- управлять взаимосвязями со всеми партнерами, поставщиками и заказчиками, которые рассматриваются как имеющие влияние на ИБ защищаемых активов;
- устанавливать контекст управления стратегическими рисками организации, в котором будут осуществляться разработка и сопровождение СУИБ;
- быть утвержденной высшим руководством организации.

После разработки и согласования Политика СУИБ утверждается руководством организации.

Также должно быть гарантировано, что все сотрудники организации и заинтересованные стороны, входящие в заявленную область действия СУИБ, ознакомлены с данной Политикой, понимают, какое влияние она оказывает на их работу, и исполняют ее. Политика СУИБ ориентирована на непосредственных ее потребителей и гарантирует им наличие работоспособной СУИБ, действительно эффективно функционирующей в организации.

Рекомендуется иметь Политику СУИБ краткую и концентрирующуюся на глобальных аспектах. В ней не должно быть конкретного и детального описания проблем и шагов, необходимых для внедрения и исполнения этой политики.

Чтобы удовлетворить всем требованиям, хорошая Политика СУИБ, как и ПолиБ, должна соответствовать целям организации, быть применимой, осуществимой для внедрения, превентивной, легкой в понимании, избегать абсолютных понятий.

Формат Политики СУИБ определяется внутри организации. Важно, чтобы она воспринималась как программный документ, который хочется прочесть, а не бегло просмотреть и проигнорировать.

Политика СУИБ должна охватывать следующие ключевые процессы СУИБ:

- управление рисками ИБ;
- управление инцидентами ИБ;
- управление аудитами ИБ;
- управление эффективностью СУИБ;
- управление персоналом;
- управление документацией и записями СУИБ;
- анализ функционирования СУИБ руководством организации;
- пересмотр и совершенствование СУИБ;
- управление корректирующими и предупреждающими действиями в области ОИБ;
- УНБ.

Как и ПолиБ, Политику СУИБ необходимо периодически пересматривать на предмет актуализации ее целей и основных положений.

Если отойти от формальных требований стандартов и задуматься, кто, кроме высшего руководства организации, обладает достаточными полномочиями для принятия перечисленных решений и выполнения перечисленных действий, то можно прийти к выводу, что только высшее руководство и в состоянии осуществлять эту деятельность, столь необходимую для полноценной жизни СУИБ. Только в таком случае появляется уверенность в том, что для СУИБ будут предоставлены все необходимые ресурсы, все управленческие решения будут также

приняты в срок и с учетом стратегических целей бизнеса организации.

Бывают случаи, когда проекты по построению СУИБ инициируются руководителями подразделений ИБ. Тогда им необходимо потратить достаточно много времени, чтобы донести до высшего руководства организации все преимущества построения СУИБ, а также очертить круг задач, которые нужно решить в ходе ее построения и эксплуатации.

Помимо этого, в рамках всех стадий жизненного цикла СУИБ потребуется постоянная работа высшего руководства и принятие дополнительных управленческих решений. Введение СУИБ в действие должно быть утверждено руководством организации, например, соответствующим приказом по организации. Для регулярного анализа результатов работы СУИБ руководство должно принимать необходимые решения по улучшению или модификации процессов управления ИБ. В рамках данного процесса на рассмотрение руководства организации выносятся результаты и вопросы функционирования СУИБ, статистика по процессам управления Ж, запросы заинтересованных сторон на внесение изменений в СУИБ и т. д. По результатам данного процесса на регулярной основе руководство организации выносит решения по всем аспектам работы СУИБ, требующим доработки. Ценность этих результатов заключается в том, что все решения, принимаемые руководством, согласованы с общей бизнес-стратегией организации. Это очень важно, так как, как уже отмечалось выше, в самом определении СУИБ подчеркивается, что СУИБ является частью общей системы управления организации и все решения, принимаемые в рамках СУИБ, должны учитывать цели и задачи бизнеса организации.

Чтобы функционировать эффективно, организация должна идентифицировать различные виды осуществляемой деятельности и управлять ими. Как было отмечено ранее, любое действие, использующее ресурсы и управляемое с целью преобразования входных данных в выходные, может рассматриваться как процесс. Применение системы процессов в организации, идентификация и взаимодействие этих процессов, а также управление этими процессами может быть названо «процессным подходом». Все это справедливо и в отношении обеспечения и управления ИБ, так как

любые действия в рамках данных видов деятельности могут рассматриваться как процессы.

К управлению ИБ применим процессный подход, который распространяется на разработку, реализацию, эксплуатацию, мониторинг, анализ, сопровождение и совершенствование СУИБ организации. Поддержание на должном уровне СУИБ требует применения такого же подхода, как и любая другая система управления. Используемая в ISO/IEC 27001 и ГОСТ Р ИСО/МЭК 27001 для описания процессов СУИБ циклическая модель PDCA предусматривает непрерывный цикл мероприятий: «планирование — реализация - проверка - совершенствование». При таком подходе к управлению ИБ особое значение придается следующему:

- пониманию требований по ОИБ организации и необходимости определить политику и цели ОИБ;
- внедрению и использованию обоснованных защитных мер для управления рисками ИБ организации в контексте общих бизнес- рисков организации;
- мониторингу и анализу результативности и эффективности СУИБ;
- постоянному совершенствованию, основанному на объективных показателях.

На текущий момент интерес к циклической модели связан прежде всего с проблемами внедрения и совершенствования современных систем управления, в частности СУИБ. Одна из основных целей внедрения СУИБ - создание таких условий в организации, когда происходит постоянный мониторинг и улучшение каждого из процессов ОИБ и смежных процессов. Взаимно усиливая друг друга, эти улучшения позволяют создать все более совершенную систему. Частным критерием улучшения каждого из процессов может служить снижение числа несоответствий, выявляемых в ходе различных проверок, таких как внутренние аудиты ИБ, мониторинг эффективности процессов и т. д. Появление несоответствий можно рассматривать как возникновение некоторой проблемы, решение которой ведет к улучшению процесса (после этого она не возникает снова), а, следовательно, и к достижению запланированных результатов, удовлетворению всех заинтересованных сторон и реализации принципа постоянного улучшения. Каждый факт появления

несоответствия должен приводить к выполнению определенной последовательности действий, а именно:

- коррекция (устранение несоответствия);
- анализ несоответствия;
- установление коренной причины его появления;
- определение корректирующих действий, направленных на устранение причины несоответствия;
- выполнение этих действий;
- анализ их результативности и эффективности.

Если же в ходе проверок удастся выявить факты, которые могут в будущем привести к возникновению несоответствий, то надо осуществить все вышеперечисленные действия, но только теперь их целью должно быть устранение причин потенциальных несоответствий.

Процессный подход к СУИБ показан на рис. 6.1. СУИБ принимает в качестве входных данных требования по ОИБ и ожидания заинтересованных сторон, и в результате ряда необходимых действий и процессов на выходе получается управляемая ИБ, которая удовлетворяет этим требованиям и ожиданиям.

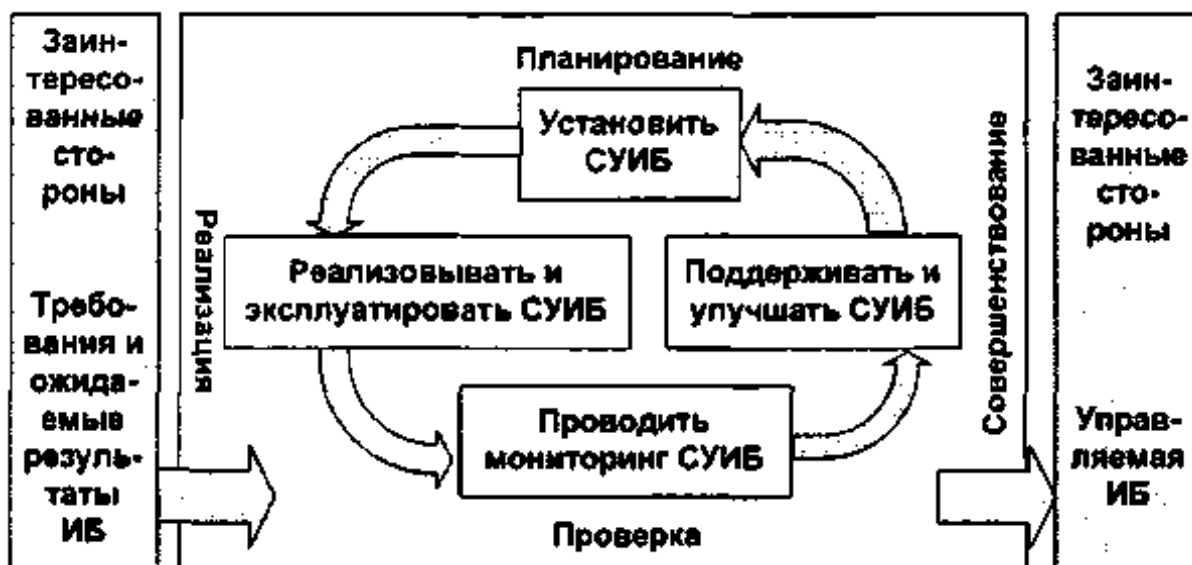


Рисунок 6.1. Цикл PDCA в применении к процессам СУИБ

На стадии планирования обеспечивается правильное задание контекста и масштаба СУИБ, оцениваются риски ИБ, предлагается соответствующий план обработки этих рисков.

На стадии реализации внедряются решения, принятые во время планирования.

Чтобы гарантировать, что СУИБ в целом достигает своих целей, необходимы периодические проверки. На стадиях проверки и совершенствования усиливают, исправляют и совершенствуют решения по СУИБ, которые были определены и уже реализованы. В зависимости от конкретной ситуации проверки СУИБ могут проводиться в любое время и с любой периодичностью. В некоторых системах с целью обеспечения немедленного выполнения и реагирования они должны быть встроены в автоматизированные процессы. Для других процессов реагирование требуется только в случае инцидентов ИБ, когда в защищаемые активы внесены изменения или дополнения или произошли изменения угроз ИБ и уязвимостей. Процесс непрерывного совершенствования обычно требует первоначального инвестирования в документирование деятельности, формализацию подхода к управлению рисками ИБ, определению методов анализа и выделению ресурсов и т. п. Эти меры используются для приведения цикла в действие. Они не обязательно должны быть завершены, прежде чем будут активизированы стадии пересмотра СУИБ.

Детально содержание деятельности в рамках названных стадий показано рис. 6.2.

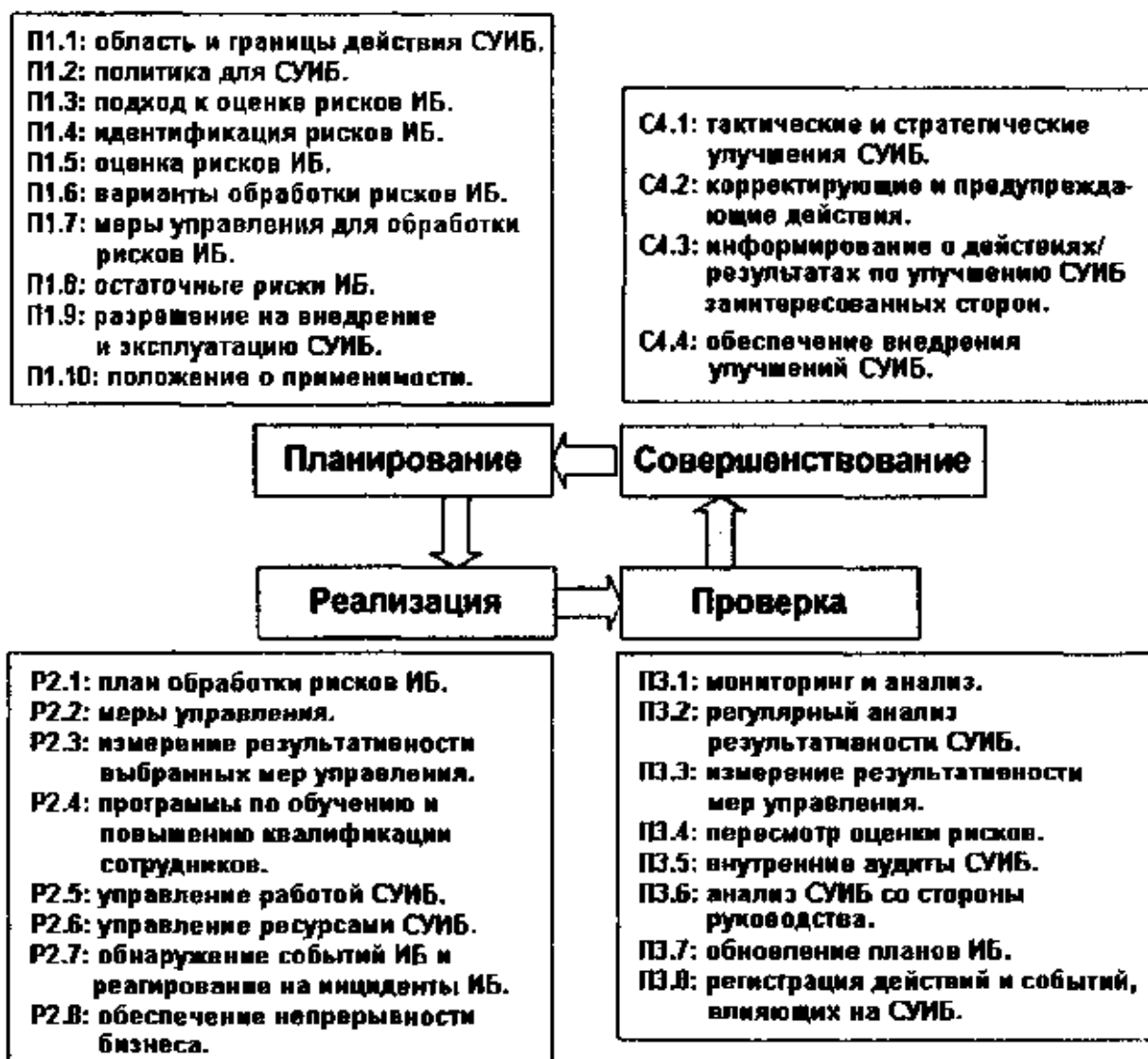


Рисунок 6.2. Процессы цикла PDCA в применении к процессам СУИБ

Планирование СУИБ

Применительно к системе управления ИБ (далее СУИБ) на этапе планирования осуществляются непосредственная ее разработка: устанавливается область действия и политика для СУИБ, определяются цели, задачи, процессы и процедуры, адекватные потребностям бизнеса в управлении рисками ИБ и позволяющие повысить уровень ИБ, а также получить результаты, соответствующие общим политикам и целям организации.

Целью выполнения деятельности в рамках группы процессов «планирование» является запуск «цикла» СУИБ путем определения первоначальных планов ее построения, ввода в действие и контроля, а также определения планов по

совершенствованию на основании решений, принятых на этапе «совершенствование» (если это уже не первый цикл).

Сочетая при создании СУИБ различные принципы управления в каждом отдельном контуре защиты объекта, можно добиться оптимального соотношения эффективности и стоимости ОИБ. Разработка СУИБ, как и любой другой системы управления, основывается на трех базовых принципах управления :

Разомкнутое управление — заранее сформированные требования реализуются исполнителями ОИБ, воздействуя на объект защиты; достоинство - простота, недостаток - низкая эффективность защиты, так как трудно заранее предугадать момент воздействия и вид угрозы ИБ.

Компенсация - в контур управления ИБ оперативно вводится информация об обнаруженной угрозе ИБ, в результате чего исполнители ОИБ концентрируют свои усилия на ее локализации и противодействии ей; достоинство - более высокая эффективность, недостатки - трудность правильного обнаружения угрозы ИБ и невозможность устранения последствий внутренних угроз.

Обратная связь - обнаруживается не сама угроза ИБ, а реакция системы на нее и степень нанесенного ущерба; достоинства - конкретность и точность отработки последствий внешних и внутренних угроз ИБ (экономическая целесообразность), недостаток - запаздывание (инерционность) принимаемых защитных мер.

Выполнение деятельности на данной стадии заключается в обследовании организации с целью определения степени соответствия требованиям по ОИБ и требованиям к СУИБ, определении/корректировке области действия СУИБ, разработке плана мероприятий по построению СУИБ с учетом выбранной области и степени соответствия требованиям к СУИБ в границах области деятельности, формализации подхода к оценке рисков ИБ и распределении ресурсов, проведении оценки рисков ИБ и определении/коррекции планов их обработки, разработке механизмов и процессов управления ИБ.

При проведении обследования организации основными источниками информации являются документы организации (политики, процедуры,

инструкции и т. д.) и результаты интервьюирования сотрудников организации. После обследования организация должна выполнить следующее:

1. Определить/уточнить область и границы действия СУИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий, также включая детали и обоснования любых исключений из области действия; при этом важно учесть все риски для организации - операционные, репутационные и т. п.

2. Определить/уточнить политику для СУИБ (она имеет приоритет по сравнению с ПолИБ организации, хотя они и могут быть представлены одним общим документом) на основе характеристик бизнеса, организации, ее размещения, активов и технологий, которая:

- включает в себя концепцию для установки целей, основных направлений и принципов действия в отношении ИБ;
- учитывает бизнес-требования и нормативно-правовые требования (включая международные и национальные стандарты в области ОИБ), а также договорные обязательства по ОИБ;
- согласуется со стратегическим управлением рисками организации, в рамках которого будет происходить разработка и поддержка СУИБ;
- устанавливает критерии оценки рисков;
- утверждается руководством.

3. Определить/уточнить подход к оценке рисков ИБ для наиболее критичных активов и бизнес-процессов организации, включая:

- методологию оценки рисков ИБ, которая применима для СУИБ и соответствует установленным бизнес-требованиям по ОИБ и нормативно-правовым требованиям; она должна давать сравнимые и воспроизводимые результаты;

- критерии принятия рисков и приемлемые уровни риска.

4. Выявить и идентифицировать риски ИБ, определив:

- защищаемые активы в рамках области действия СУИБ, а также владельцев этих активов;
- угрозы ИБ для этих активов;
- уязвимости активов, которые могут быть использованы угрозами ИБ;

- негативные последствия, которые ведут к потере конфиденциальности, целостности и доступности активов.

5. Проанализировать и оценить риски ИБ, для чего необходимо оценить:

- ущерб для деятельности организации, который может быть нанесен в результате сбоя в ОИБ, с учетом возможных последствий нарушения конфиденциальности, целостности или доступности активов;

- реальную вероятность сбоя в ОИБ с учетом превалирующих угроз, уязвимостей и их последствий, связанных с этими активами, а также применяемых на текущий момент мер управления ИБ;

- уровни рисков;
- являются ли риски приемлемыми или требуют обработки с использованием критериев приемлемых рисков.

6. Определить и оценить различные варианты обработки рисков ИБ, среди которых:

- применение подходящих мер управления;
- сознательное и объективное принятие рисков при условии, что они полностью соответствуют требованиям политики и критериям организации в отношении принятия рисков;

- избежание риска;
- передача соответствующих бизнес-рисков сторонним организациям, например, страховщикам или поставщикам.

7. Выбрать цели и меры управления (защитные меры) для обработки рисков ИБ, которые должны удовлетворять требованиям, определенным в процессе оценки и обработки рисков, с учетом критериев принятия рисков и нормативно-правовых требований и договорных обязательств.

8. Получить утверждение руководством предлагаемых остаточных рисков ИБ.

9. Получить разрешение руководства на внедрение и эксплуатацию СУИБ.

10. Подготовить Положение о применимости, которое включает следующее:

- цели и меры управления и обоснование этого выбора;
- цели и меры управления, реализованные в настоящее время;

- перечень исключений целей и мер управления и процедуру обоснования их исключения.

Фактически представленные шаги этапа планирования СУИБ преследуют цель принятия решения организацией по следующим трем основным вопросам:

1) установление области действия и политики СУИБ (шаги 1 и 2);

2) выбор защитных мер на основе управления рисками ИБ (шаги 3—7);

3) получение одобрения руководства для мер обработки рисков ИБ и подготовка формулировки применимости требований, так как это влечет организационные и, возможно, финансовые издержки организации (шаги 8-10).

Все перечисленные действия являются весьма объемными и трудоемкими. Для их выполнения необходимо создание рабочей группы специалистов из разных подразделений организации, обладающих достаточными знаниями и полномочиями для принятия управленческих решений на всех этапах построения и последующего внедрения СУИБ.

Помимо этого необходимо, чтобы руководство организации было также заинтересовано в построении СУИБ. Важно, чтобы все решения на этапе «планирование» были поддержаны и приняты руководством организации. Приверженность руководства может существенно облегчить разработку и внедрение системы.

Выходом данного этапа являются разработанные процессы управления ИБ, процедуры, поддерживающие и обеспечивающие работу разработанных процессов, а также инструкции для пользователей процессов и исполнителей ролей в рамках процессов.

Реализация СУИБ

На этапе реализации СУИБ происходит внедрение системы и разработанных процессов управления ИБ и последующая их эксплуатация, а именно: внедрение и применение политики в отношении СУИБ, защитных мер, процессов и процедур СУИБ. Это весьма трудоемкий процесс, так как он требует назначения исполнителей ролей участников разработанных процессов и проведения обучения исполнителей работ, может требовать оперативной корректировки процессов и т. д.

Этап «реализация» осуществляется по результатам выполнения этапов «планирование» и/или «совершенствование» и заключается в выполнении всех планов, связанных с построением, вводом в действие и совершенствованием СУИБ, определенных на этапе «планирование», и/или реализации решений, определенных на этапе «совершенствование» и не требующих выполнения деятельности по планированию соответствующих улучшений. Среди прочего важным является выполнение таких видов деятельности, как организация обучения и повышение осведомленности в области ИБ, реализация обнаружения и реагирования на инциденты ИБ, ОНБ.

Организация должна выбирать защитные меры, адекватные моделям угроз и нарушителей ИБ, с учетом затрат на реализацию таких мер и объема возможных потерь от реализации угроз ИБ. Должны применяться только те защитные меры, правильность работы которых может быть проверена. При этом организация должна регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на бизнес-цели.

Для реализации СУИБ организация должна предпринять следующее:

а) разработать план обработки рисков ИБ, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении управления рисками ИБ;

б) реализовать план обработки рисков ИБ для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределения функций и обязанностей;

в) внедрить меры управления для достижения целей управления;

г) определить способ измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления с целью получения сравнимых и воспроизводимых данных;

д) реализовать программы по обучению и повышению квалификации сотрудников;

е) управлять работой СУИБ;

ж) управлять ресурсами СУИБ;

з) внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты ИБ;

и) обеспечить непрерывность бизнеса организации.

Подробно поэтапные действия по внедрению СУИБ, составленные в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001, ISO/IEC 27001 и немецкой методикой IT-Grundschutz, выглядят следующим образом:

Этап 1 -управленческий:

- осознать цели и выгоды внедрения СУИБ;
- получить поддержку руководства на внедрение и ввод в эксплуатацию СУИБ;
- распределить ответственность по СУИБ.

Этап 2 - организационный:

- создать и обучить группу по внедрению и поддержке СУИБ;
- определить область действия СУИБ.

Этап 3 — первоначальный анализ существующей СУИБ:

- провести анализ СУИБ;
- определить перечень работ по доработке СУИБ.

Этап 4 — определение Политики СУИБ и целей СУИБ по каждому процессу.

Этап 5 — сравнение текущей ситуации со стандартом 27001:

- провести обучение требованиям стандарта ответственных за СУИБ;
- сравнить требования стандарта с существующим положением дел.

Этап 6 — планирование внедрения СУИБ:

- определить перечень мероприятий для достижения требований стандарта;
- разработать руководство по ИБ.

Этап 7 - внедрение системы управления рисками ИБ:

- разработать процедуру идентификации рисков ИБ;
- идентифицировать и ранжировать активы (каталог «Модули» методики IT-Grundschutz);
- определить ответственных за активы;
- оценить активы;

- идентифицировать угрозы ИБ и уязвимости активов (каталог «Угрозы» методики);
- рассчитать и ранжировать риски ИБ;
- разработать план по снижению рисков ИБ (каталог «Защитные меры» методики);
- определить неприменимые средства управления ИБ (приложение А стандарта 27001);
- разработать положение о средствах управления ИБ.

Этап 8 —разработка документации СУИ Б:

- определить перечень документов (процедур, записей, инструкций) для разработки;
- разработать следующие процедуры и другие документы:
 - 1) управленческие процедуры (стандарт на разработку документов, управление документами и записями; корректирующие и предупреждающие мероприятия; внутренний аудит ИБ; управление персоналом и т. д.);
 - 2) технические процедуры (приобретение, развитие и поддержка ИС; управление доступом; регистрация и анализ инцидентов ИБ; резервное копирование; управление съемными носителями и т. д.);
 - 3) управленческие записи (отчеты о внутренних аудитах ИБ; анализ СУИБ со стороны высшего руководства организации; отчет об анализе рисков ИБ; отчет о работе комитета по ИБ; отчет о состоянии корректирующих и предупреждающих действий; договоры; личные дела сотрудников и т. д.);
 - 4) технические записи (реестр активов; план предприятия; план физического размещения активов; план компьютерной сети; журнал регистрации резервного копирования; журнал регистрации факта технического контроля после изменений в ОС; журнал событий ИС; журнал регистрации действий системного администратора; журнал регистрации инцидентов ИБ; журнал регистрации тестов по непрерывности бизнеса и т. д.);
 - 5) инструкции, положения (правила работы с компьютерами и ИС, правила обращения с паролями, инструкция по восстановлению данных из резервных копий, политика удаленного доступа, правила работы с переносным оборудованием и т. д.); введение в действие документов СУИБ.

Этап 9 - обучение персонала требованиям ИБ (руководителей, сотрудников).

Этап 10 — разработка и принятие мер по обеспечению работы СУИБ: внедрение средств защиты (административных, программно-аппаратных, технических).

Этап 11 - внутренний аудит СУИБ: подбор команды, планирование и проведение.

Этап 12 - анализ СУИБ со стороны высшего руководства.

Этап 13 - официальный запуск СУИБ: приказ о введении в действие СУИБ.

Этап 14 - оповещение заинтересованных сторон: информирование клиентов, партнеров, СМИ о запуске СУИБ.

Важным фактором успешного внедрения СУИБ является создание рабочей группы, ответственной за внедрение СУИБ. В ее состав должны войти:

- представители высшего руководства организации;
- представители подразделений, охватываемых СУИБ;
- специалисты подразделений, обеспечивающих ИБ в организации, имеющие соответствующее образование или подготовку, знающие основные принципы и лучшие практики в области ИБ.

Перечисленные сотрудники должны понимать защитные меры и процессы СУИБ, знать требования нормативной и правовой базы, поддерживаемой в организации, и пройти обучение по вопросам создания и эксплуатации СУИБ. В состав рабочей группы могут также входить привлеченные консультанты, специализирующиеся в вопросах СУИБ. Хорошей практикой является создание в организации комитета по ИБ, который, кроме вопросов, связанных с внедрением СУИБ, должен на постоянной основе обеспечить решение задач, определяемых эксплуатацией данной СУИБ и ее непрерывным совершенствованием.

Процедуры для реализации и управления СУИБ могут быть организованы как система (дерево) процессов (в терминах процессного подхода). Отдельные шаги реализации СУИБ могут быть организованы как целевые (профильные) процессы деятельности, иницируемые и завершаемые по принятым для них критериям (по времени или событию) и имеющие собственные самостоятельные регламентирующие нормы, включая

организационную и ресурсную поддержку. Это может быть также следствием решений организации в результате реализации требований нескольких стандартизированных систем управления (не только стандартной СУИБ, но и иных стандартизированных направлений управления). Поскольку практически все международные стандарты на системы управления методологически совместимы, это позволяет выделять и поддерживать унифицированные задачи, например, в части работы с персоналом организации, регистрации и сбора индентов и т. п.

Проверка СУИБ

Вопросы реализации СУИБ на практике неотделимы от соответствующих процедур контроля, сформулированных в отдельном блоке требований СУИБ. На этапе проверки производятся мониторинг и анализ СУИБ, включающие оценку и, если возможно, количественное измерение результативности и эффективности процессов для проверки соответствия требованиям политики, целям ОИБ и практическому опыту функционирования СУИБ, а также информирование высшего руководства организации о результатах для последующего анализа.

Целью выполнения деятельности в рамках группы процессов «проверка» является обеспечение достаточной уверенности в том, что СУИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам ИБ, а также внутренним и/или внешним условиям функционирования организации, влияющим на ИБ. Кроме того, необходимо рассмотреть любые изменения в допущениях или области оценки рисков ИБ. Организация должна своевременно обнаруживать проблемы, прямо или косвенно относящиеся к ИБ, потенциально способные повлиять на ее бизнес-цели. Рекомендуются выявлять причинно-следственную связь возможных проблем и строить на этой основе прогноз их развития. Указанная деятельность может проводиться в любое время и с любой частотой, в зависимости от того, что является подходящим для конкретной ситуации.

На этапе «проверка» необходимо осуществлять мониторинг и контроль используемых защитных мер, проводить аудит ИБ (внутренний и внешний), анализировать функционирование СУИБ в целом, в том числе со стороны руководства. Желательно

интегрировать процессы мониторинга и анализа СУИБ в систему внутреннего контроля организации.

Результат выполнения деятельности на этапе «проверка» является основой для выполнения деятельности по совершенствованию СУИБ.

Согласно более детально для проверки СУИБ организация должна предпринять следующее:

1. Выполнять процедуры мониторинга и анализа, а также использовать другие средства управления в следующих целях:

- способствовать своевременному выявлению событий ИБ (ошибок в обработке информации, удавшихся и неудавшихся попыток нарушения ИБ) и, таким образом, предотвращать инциденты ИБ путем применения средств индикации;

- предоставлять руководству информацию для принятия решений о ходе выполнения деятельности по ОИБ, осуществляемой как ответственными лицами, так и ИТ;

- определять, являются ли эффективными действия, предпринимаемые СУИБ для устранения нарушений ИБ.

2. Проводить регулярный анализ результативности СУИБ (включая проверку ее соответствия политике и целям СУИБ и анализ мер управления ИБ) с учетом результатов аудиторских проверок ИБ, инцидентов ИБ, результатов измерений эффективности СУИБ, а также предложений и другой информации от всех заинтересованных сторон.

3. Измерять результативность средств управления для проверки соответствия требованиям по ОИБ.

4. Пересматривать оценки рисков ИБ через оговоренные периоды времени, анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения в организации, технологиях, целях деятельности и процессах, выявленных угрозах ИБ, результативности реализованных мер управления и внешних условиях, например, изменения нормативно-правовых требований, договорных обязательств, а также изменения в социальной структуре общества.

5. Проводить внутренние аудиты СУИБ через установленные периоды времени.

6. Регулярно проводить руководством организации анализ СУИБ в целях подтверждения адекватности ее функционирования

в рамках установленной области действия и определения направлений совершенствования.

7. Обновлять планы ОИБ с учетом результатов анализа и мониторинга.

8. Регистрировать действия и события, способные повлиять на результативность или функционирование СУИБ.

Совершенствование СУИБ

Группа процессов «совершенствование» включает в себя деятельность по принятию решений о реализации тактических и/или стратегических улучшений СУИБ. Переход к этому этапу осуществляется только тогда, когда выполнение процессов этапа «проверка» дало результат, требующий совершенствования СУИБ. При этом сама деятельность по совершенствованию СУИБ должна реализовываться в рамках групп процессов «реализация» (например, введение в действие существующего плана ОНБ, поскольку на стадии «проверка» определена необходимость в этом) и при необходимости «планирование» (идентификация новой угрозы ИБ и последующие обновления оценки рисков на стадии «планирование»). При этом важно, чтобы все заинтересованные стороны немедленно извещались о проводимых улучшениях СУИБ и при необходимости проводилось соответствующее обучение.

Реализация и внедрение данного процесса позволяет достичь следующих целей:

1) в организации действует механизм непрерывного улучшения СУИБ в целом и отдельных ее процессов;

2) все выявленные или прогнозируемые отклонения показателей функционирования СУИБ от нормальных значений учитываются и предпринимаются действия для исправления ситуации.

Основной задачей данного процесса является предупреждение и устранение причин несоответствий - ситуаций, когда процессы или меры по ОИБ не соответствуют требованиям, заданным законодательством, международными стандартами, нормативно-распорядительными или иными документами, регламентирующими вопросы ОИБ в рамках области действия СУИБ организации. Более детально для совершенствования СУИБ организация должна выполнять следующее:

а) выявлять возможности тактического и стратегического улучшений СУИБ;

б) предпринимать корректирующие и предупреждающие действия, использовать на практике опыт по ОИБ, полученный как в самой организации, так и в других организациях;

в) передавать подробную информацию о действиях/результатах по улучшению СУИБ всем заинтересованным сторонам, при этом степень детализации должна соответствовать обстоятельствам и при необходимости согласовывать дальнейшие действия;

г) обеспечивать внедрение улучшений СУИБ для достижения запланированных целей.

На этапе совершенствования СУИБ с целью обеспечения ее непрерывности производится разработка и внедрение корректирующих и превентивных (предупреждающих) действий по результатам внутреннего аудита и анализа СУИБ, выполненного руководством организации, а также на основе другой значимой информации. Корректирующее действие - действие, предпринятое для устранения причины обнаруженного несоответствия. Предупреждающее действие - действие, предпринятое для устранения причины потенциального несоответствия или другой потенциально нежелательной ситуации. Корректирующее действие предпринимается для предотвращения повторного возникновения несоответствия, тогда как предупреждающее действие - для предотвращения возникновения несоответствия. Действие по предупреждению несоответствий часто является экономически более выгодным, чем корректирующее действие.

При корректировке функционирования СУИБ в первую очередь устраняются несоответствия двух видов:

1) отсутствие или невозможность реализации некоторых требований СУИБ;

2) неспособность СУИБ обеспечить соблюдение ПолиБ или реализовывать бизнес-цели организации.

Документированная процедура для корректирующего и предупреждающего действия должна определять требования для следующего:

- выявление несоответствий (имеющихся и возможных);
- определение причин несоответствий;

- оценивание потребности в действиях, чтобы гарантировать, что несоответствия не возникнут снова;
- определение и реализация требующихся действий;
- записывание результатов предпринятых действий;
- анализ предпринятого действия.

Организация должна определить и предпринять действия по устранению причины (включая определение изменившихся рисков) несоответствия требованиям СУИБ. Причины несоответствий могут быть разделены на следующие группы:

- организационные недостатки;
- ошибки персонала;
- технические сбои;
- злоумышленные действия;
- обстоятельства непреодолимой силы.

Выявление и прогноз несоответствий защитных мер и процессов по управлению ИБ осуществляют, как правило, владельцы бизнес- процессов и лица, ответственные за эксплуатацию средств защиты. Несоответствия могут быть выявлены также любыми сотрудниками организации. Лицо, выявившее или спрогнозировавшее несоответствие, сообщает об этом, как правило, ответственному лицу, которое оформляет данный факт в виде необходимой записи СУИБ.

Источниками информации по выявленным или прогнозируемым несоответствиям могут являться:

- отчеты о внутренних и внешних аудитах ИБ;
- жалобы и рекомендации пользователей организации;
- результаты анализа функционирования СУИБ руководством;
- результаты мониторинга эффективности СУИБ;
- данные по инцидентам ИБ;
- любая другая информация, указывающая на наличие действующих или потенциальных несоответствий.

Записи о несоответствиях или о потенциальных несоответствиях должны регистрироваться. При регистрации несоответствия лучше группировать по некоторым категориям, например, в соответствии с тем, к какому процессу управления ИБ или к какой группе защитных мер относится несоответствие. Это

может оказаться полезным для последующего анализа статистики корректирующих и предупреждающих действий.

В разработке (а потом и организации выполнения) корректирующего или предупреждающего действия принимают участие владелец процесса СУИБ или руководитель структурного подразделения, в процессе (подразделении) которого возможно возникновение или возникло несоответствие. Руководитель подразделения по своему усмотрению может назначить одного из сотрудников подразделения ответственным за внедрение предупреждающего действия.

При разработке корректирующих или предупреждающих действий обязательно проводится оценка необходимости и адекватность затрат на проведение этих действий.

При этом должны учитываться следующие факторы:

- документ или требование, к которому относится данное несоответствие;
- причины несоответствий в процессе;
- целесообразность разработки корректирующих или предупреждающих действий;
- сроки выполнения корректирующих или предупреждающих действий;
- сроки проверки эффективности корректирующего / предупреждающего действия;
- ответственность за выполнение действия и проверку его эффективности.

Решение о предупреждающем или корректирующем действии принимается только при условии, если это действие не влияет на целостность СУИБ. Действие признается нарушающим целостность СУИБ, если его выполнение влечет за собой:

- несоответствие требованиям внутренних и внешних нормативных документов;
- нарушение требований документации СУИБ;
- снижение эффективности организационной структуры из-за появления у подразделений задач, дублирующих существующие, или появление участков с неопределенной ответственностью;
- нарушение баланса между ответственностью и полномочиями.

По результатам выполнения корректирующего или предупреждающего действия в сроки, установленные при планировании этого действия, осуществляется контроль эффективности его выполнения.

Работа с процессами СУИБ организации

Как было показано выше, в рамках процессного подхода к управлению ИБ и циклической модели PDCA постоянно приходится оперировать понятием процесса. Поэтому целесообразно определить основные способы задания и анализа процессов управления ИБ организации, реализуемых в рамках всего жизненного цикла СУИБ (для краткости называемых далее процессами СУИБ). Эти процессы затрагивают все аспекты ОИБ организации, так как ИБ — это результат устойчивого функционирования системы защиты ИС. Рассмотрим две названные стратегии внедрения СУИБ более подробно.

Построение и внедрение СУИБ в целом

Построение и внедрение СУИБ в целом является трудоемкой задачей, так как на этапе разработки требуется отследить все взаимосвязи между процессами управления ИБ, а также сконструировать большое количество процессов таким образом, чтобы они заработали эффективно.

Объемы и сложность решаемых задач требуют слаженной работы целой команды специалистов. При построении СУИБ, внедряемой по данной схеме, необходимо организовать рабочую группу, которая будет включать в себя специалистов в разных областях: специалистов по ИБ, владельцев бизнес-процессов (как правило, это линейные руководители подразделений), специалистов по информационно-технологической поддержке, специалистов по кадрам, представителей финансового подразделения и т. д. Помимо этого необходимо не забывать про роль высшего руководства в этом процессе.

Как правило, при данной схеме внедрения СУИБ большой объем работ идет параллельно. При внедрении СУИБ в целом осуществляется разработка и практически одновременное внедрение перечисленных ранее процессов управления ИБ, реализуемых в рамках функционирования СУИБ: управление рисками ИБ, инцидентами ИБ и т. д. (п. 4.7). В такой ситуации

важную роль играют грамотное планирование работ и их хорошая координация.

Для построения ряда процессов необходимо соблюдать определенную последовательность. Так, после утверждения области действия будущей СУИБ и разработки Политики СУИБ необходимо приступить к анализу рисков ИБ. И только после получения результатов работы данного процесса — отчета по результатам анализа рисков ИБ и плана обработки рисков ИБ — можно приступить к разработке необходимых процессов и процедур, учитывающих, если это необходимо, планируемые защитные меры. Далее, поскольку в рамках СУИБ создается достаточно большое количество документов, а по процессам управления ИБ создаются записи, еще на ранних стадиях разработки СУИБ необходимо разработать и внедрить функционирующие под ее контролем процессы управления документами и записями. После этого можно приступить к разработке группы процессов анализа и улучшения СУИБ (внутренние аудиты ИБ; мониторинг эффективности процессов и защитных мер; управление корректирующими/предупреждающими действиями), а также процессов управления инцидентами ИБ и УНБ. Все эти процессы будут подробно рассмотрены далее.

При выборе стратегии внедрения СУИБ в целом тоже существуют различные варианты ее построения, которые в основном затрагивают аспекты выбора области действия. Существует две возможности - внедрение СУИБ для небольшой (ограниченной) области действия с последующим расширением или сразу для всей области действия.

СУИБ для небольшой области действия с последующим расширением

В качестве области действия СУИБ может быть выбран небольшой (в смысле не сложный) процесс, в котором участвует небольшое количество сотрудников. Основными преимуществами такого подхода являются:

- возможность более легкой модификации процессов управления ИБ на этапе их внедрения;
- более тесная работа с сотрудниками, входящими в область действия СУИБ, в части внедрения процессов управления ИБ в культуру организации;

- оперативная связь с сотрудниками в ходе внедрения процессов управления ИБ;
- использование данной области действия в качестве «испытательного полигона» для отработки всех процессов управления ИБ.

Проект по построению СУИБ для небольшой области действия занимает меньше времени и требует на первых этапах менее тщательной отработки всех процессов. Помимо этого, данная область, как было сказано выше, может быть использована в качестве полигона - процессы, разработанные в рамках данной области действия, могут быть использованы впоследствии в качестве шаблонов при расширении области действия СУИБ на другие процессы. В рамках последующих проектов по расширению области действия СУИБ могут быть использованы отработанные методики анализа рисков ИБ, обработки инцидентов ИБ, обучения сотрудников и т. д. При этом совершенно необязательно расширять зону действия всех процессов управления ИБ одновременно. Возможно постепенное ее расширение, начиная с тех процессов, которые уже хорошо отработаны на полигоне и могут принести существенную пользу при своем расширении.

Из аспектов, которые требуют особого внимания при расширении области действия СУИБ, выделим то, что при принятии решения о добавлении в область действия СУИБ новых активов (бизнес-процессов) организации, нужно четко определить цели расширения СУИБ на них и цели самой СУИБ в рамках данных активов. Следует также отметить, что расширение единой СУИБ возможно и на смежные активы. Если рассматривать отдельные, невзаимосвязанные процессы, то, скорее всего, нужно внедрять разные локальные СУИБ.

СУИБ для большой области действия

Построение СУИБ сразу для большой области действия обладает рядом своих преимуществ и недостатков. Из преимуществ можно выделить то, что если такой проект реально запускается, то, скорее всего, имеется действительная заинтересованность руководства в нем и для построения и внедрения СУИБ все управленческие решения будут приниматься своевременно, а все необходимые ресурсы предоставляться вовремя.

Но при таком подходе на этапах внедрения и дальнейшего функционирования СУИБ практически невозможно оперативно вносить изменения в процессы управления ИБ. Это обусловлено тем, что такие процессы чаще всего затрагивают большое количество сотрудников. Их оповещение и обучение новым правилам - не такая простая задача. Помимо этого в связи с обширностью области действия, управленческая ролевая структура, скорее всего, будет весьма разветвленной и негибкой, что повлечет за собой сложности в согласовании вносимых изменений. Механизмы получения обратной связи от пользователей СУИБ также не будут такими простыми и гибкими, как в случае внедрения СУИБ на небольшой области действия.

Однако подход, при котором СУИБ охватывает большую часть организации, может свидетельствовать о серьезном подходе руководства организации к ОИБ и управлению ею.

Построение и внедрение процессов СУИБ по отдельности

При построении и внедрении процессов управления ИБ, выполняемых в рамках функционирования СУИБ, можно выделить те же преимущества, что и для СУИБ для небольшой области действия. Однако ошибочно думать, что эти преимущества достигаются только лишь при внедрении отдельных процессов для небольшой области действия. Если внедрять процессы постепенно, то этих же преимуществ можно добиться и при внедрении сразу же для большой области действия.

При выборе стратегии внедрения процессов СУИБ по отдельности с последующим их объединением в СУИБ последовательность работ и разработки и внедрения процессов будет примерно такой же, как и при внедрении СУИБ в целом. За исключением того, что цели внедрения отдельных процессов должны определяться на этапе их разработки и потом их выполнение должно четко отслеживаться. Возможно, потребуется оформление политик для каждого из процессов, которые будут по структуре совпадать со структурой общей политики СУИБ.

При внедрении отдельных процессов необходимо делать это постепенно, отводя время на внедрение процесса в культуру, обучение пользователей, внесение изменений в процесс по результатам первых циклов его работы. Именно в таком случае

будут достигнуты преимущества данной стратегии внедрения СУИБ.

Из недостатков стратегии отметим следующее. Поскольку процессы будут разрабатываться отдельно, возможно разными людьми, то при их постепенном внедрении и последующем объединении в единую систему могут возникнуть проблемы с взаимосвязями между процессами. Это может быть вызвано несоответствием выходных данных одного процесса и входных данных следующего за ним процесса управления ИБ, несоответствием ролей и исполнителей ролей в разных процессах и т. д. Чтобы избежать этого, необходимо иметь четкую стратегию развития процессов и СУИБ в целом, последовательно ее отслеживать и строить СУИБ в соответствии с ней.

6.2. Современные и перспективные российские аппаратные, программные и аппаратно-программные комплексы технического противодействия компьютерной разведке, их назначение и функциональные возможности

На волне импортозамещения, а также с учетом угроз руководства США нанести ответный «кибер-удар» по России в сфере обеспечения безопасности стали активно появляться российские разработки и решения. Проведем обзор аппаратно-программных решений, завоевавших признание государственных структур, только одной из многих российских компаний, но входящей в Топ-10 лучших мировых компаний сферы ИБ – ЗАО «Норси-Транс», продукцию которой западные аналитики называют электронным «автоматом Калашникова» за мощность и надежность. ЗАО «Норси-Транс» 20 лет на рынке аппаратно-программных решений для силовых структур и крупных корпоративных клиентов.

Комплекс регистрации операций и потоков данных в информационных системах «ЛАНГРАФ – С»

«Ланграф-С» предназначен для использования в комплексах защиты информации. Повышает эффективность противодействия внутренним угрозам информационной безопасности.

Функции комплекса:

- Анализ и протоколирование действий пользователя информационной системы при обмене данными с внешними накопителями (Floppy, USB Flash/HDD, SCSI MO, CD/DVD R/RW);
- Пассивный анализ и протоколирование сетевых потоков данных при работе пользователя с СУБД, Интернет и другими информационными ресурсами;
- Анализ и протоколирование операций печати на локальных или сетевых принтерах с рабочих мест пользователей;
- Сбор и обработка информации о состоянии рабочих мест пользователей и локальной сети в целом;
- Хранение и обеспечение доступа к сохранённым элементам информационных потоков.

Базовый состав:

- Монитор сети;
- Сервер статистики;
- Сервер хранения;
- Рабочее место сотрудника безопасности;
- Набор локальных компонентов мониторинга компьютера пользователя ИС.

Комплекс разработан с возможностью масштабирования и обслуживания различных распределенных сетей.

Технические характеристики:

- Поддерживаемые устройства для наблюдения:
- накопители данных формата USB Flash;
- жесткие диски, подключаемые по интерфейсу USB или Firewire;
- гибкие магнитные или магнитооптические диски, как встроенные в систему, так и подключаемые по интерфейсу USB или SCSI;
- устройства записи на оптические носители CD/DVD, как встроенные в систему, так и подключаемые по интерфейсу USB, SCSI или Firewire;
- локальные устройства печати, подключаемые по интерфейсу USB или LPT;
- сетевые устройства печати, использующие протокол RAW или LPR;

- сервер сетевой базы данных Oracle для мониторинга запросов к базе;
- компьютеры локальной сети для мониторинга их состояния.
- Поддерживаемые форматы данных:
- задания печати в форматах EMF, PS, PCL, TEXT;
- образы дисков формата ISO9660/Joliet, записанные в режимах MODE1 и 2/XA, в том числе в мультисессионном режиме;
- сетевые сессии запросов к СУБД Oracle;
- прочие данные, включая документы Microsoft Office, графические изображения в форматах jpg, bmp, png, gif и др., мультимедийные файлы в форматах wav, avi, wmf и др.;
- тип операционной системы наблюдаемого компьютера – Windows 2003/XP.

Монитор сети обеспечивает высокую производительность регистрации данных с нулевой дополнительной нагрузкой на СУБД, Интернет или другой информационный ресурс; защищенность от несанкционированного доступа за счет пассивного подключения.

Рабочее место сотрудника безопасности обеспечивает отображение информации в различных режимах, сигнализацию о фактах несанкционированного доступа (далее – НСД). Реализована гибкая система фильтров, используемая для отбора искомой информации, а также набор встроенных средств визуализации сохранённых элементов данных.

"Виток-МЭ4" - передовая российская разработка в области фильтрации сетевого трафика в сетях 10G-40G-100G.

Для решения большинства задач платформа "Виток-МЭ4" производит только аппаратный анализ и передачу данных, благодаря чему не использует ресурсы CPU и способна годами работать в режиме "без потерь" (zero-loss). Поддержка сложных сетевых стеков и конфигураций, расширенный функционал и обновления могут быть поставлены Заказчику в виде прошивок производства ПАО "НОРСИ-ТРАНС".

"Виток-МЭ4" имеет Сертификат Соответствия ФСТЭК России, а также соответствует "Системам сертификации средств

защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00".

Проводимая при сертификационных испытаниях проверка функциональности "Виток-МЭ4", предназначенного для защиты от несанкционированного доступа к информации, подтвердила его соответствие требованиям руководящего документа "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" (Гостехкомиссия России, 1997) – для 4 класса защищенности.

Функционал:

- управление 12/24 10G/1G Ethernet портами, расширения 40G и 100G;

- фильтрация на сетевом уровне. Решение по фильтрации может приниматься независимо для каждого сетевого пакета на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов;

- фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

- фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

- фильтрация с учетом любых значимых полей сетевых пакетов.

"Виток-МЭ4" реализует функции по обеспечению целостности программных конфигураций межсетевого экрана и данных, хранящихся как в оперативной, так и во flash-памяти, а также предусматривает процедуру восстановления после сбоев и отказов оборудования, обеспечивающую восстановление аппаратно-программных свойств решения.

В части регистрации событий "Виток-МЭ4" обеспечивает логирование сессий административного доступа к межсетевому экрану с указанием:

- времени и даты осуществления административного доступа;

- результата попытки осуществления административного доступа – успешный или неуспешный;

- имен пользователей, использованных при попытках осуществления административного доступа;

- возможность регистрации и учета фильтруемых пакетов с указанием адреса, времени и результата фильтрации.

Электронные и электрические параметры:

- стандарт Ethernet 10G: 802.3ae;
- стандарт Ethernet 40G/100G: 802.3ba;
- порты 1G/10G (с 1 по 24);
- поддерживаемые стандарты: 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 1000BASE-SX, 1000BASE-LX, 1000BASE-EX;
- подключение к линии связи с использованием SFP/SFP+ модулей;
- управление устройством: системный порт, стандарт 10/100/1000BASE-T;
- удаленное управление устройством: WEB/HTTPS;
- потребляемая мощность: 100-200W;
- питание redundant: 220V 50Hz;
- форм-фактор: 1RU;
- опциональное подключение интерфейсов 40G и 100G Ethernet;
- потребление 1RU до 200W;
- гарантированная пропускная способность более 480 Гбит/сек в 1RU;
- канальная обработка данных без жестких дисков, процессоров и ОС;
- максимальная пропускная способность, Гбит/с: 480;
- количество параллельных сессий: не ограничено;
- количество правил таблиц фильтрации – на устройство: до 3072;
- количество правил таблиц фильтрации – на порт ввода/вывода: до 256;
- встроенные порты ввода/вывода: 12 портов 1GbE/10GbE (SFP+);
- дополнительные порты ввода/вывода: 12 портов 1GbE/10GbE (SFP+);
- встроенные порты управления: 2 порта 10/100/1000MbE UTP;
- количество VLAN, назначаемых устройством: не более 64;
- масштабируемость: поддерживается;
- дополнительный источник питания: поддерживается.

«КРОЗ» – комплексное решение для обеспечения законности в сетях операторов связи и Интернет-провайдеров (подробная информация о продукте: www.kroznet.ru)

Комплекс «КРОЗ» предназначен для решения следующих задач:

- активное решение DPI-анализа для встраивания в каналы оператора связи (совместим с оборудованием стандартов Ethernet и STM);

- обеспечение деятельности оператора связи в соответствии с законами РФ в области связи (о внедрении СОПМ, о противодействии экстремистской деятельности, о защите детей от информации, причиняющей вред их здоровью и развитию, о защите интеллектуальных прав в информационно-телекоммуникационных сетях);

- сертифицированный аппаратный комплекс, устанавливаемый в существующие каналы, не требующий изменений и не создающий узких мест в сети. Возможные схемы подключения: в разрыв канала или захват трафика по BGP;

- управление трафиком по правилам со 2 по 7 уровень модели OSI;

- интересующее заказчика наращивание функционала и возможности последующего его расширения на существующем оборудовании;

- возможности расширения спектра услуг, предоставляемых оператором связи.



В соответствии с законом от 28 июля 2012 г. №139-ФЗ «О внесении изменений в ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельными законодательными актами РФ» об ограничении доступа к ресурсам сети Интернет, содержащим информацию, распространение которой в РФ запрещено, оператор обязан блокировать доступ в соответствии с реестром запрещенных URL, доменов и сайтов.

Решение «KPO3» разработано в соответствии с Федеральным законом от 27 июля 2006 года №149-ФЗ "Об информации, информационных технологиях и о защите информации", Приказом Роскомнадзора от 17.07.2014 №103 "Об утверждении Порядка предоставления операторами связи технических средств контроля за соблюдением операторами связи требований Федерального закона от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Функционал комплекса:

- автоматизированное обновление из реестра (в том числе Реестр РосКомНадзора, ресурсы из списка Минюста) и блокировка URL;

- подробная статистика по заблокированным URL (по каждой попытке доступа), возможность экспорта;
- корректная проверка URL, включая все альтернативные формы записи;
- возможности HTTP-перенаправления или отправка информационной HTML-страницы о блокировании URL;
- межсетевой экран, задание правил по блокированию, разрыву TCP-соединений, перенаправлению, подсчету статистики или пропуску трафика. Правила включают набор элементов:
 - канальный уровень: MPLS, VLAN, длина пакета;
 - сетевой уровень: адреса сетей, географическое положение, протокол, TTL, TOS;
 - транспортный уровень: набор портов, TCP-флаги;
 - уровень приложений: HTTP URL, FTP URL, DNS NAME/CNAME;
- защита от сетевых атак как услуга в сети оператора связи и Дата-центров;
- общепринятые методы фильтрации (защита канала, TCP/IP стека сервера и уровня приложений);
- собственные инновационные методы борьбы с DoS/DDoS атаками (и оптимизация клиентских запросов для снижения нагрузки на сервер);
- возможность автоматизированного режима, не требующего вмешательства человека (подходит для фильтрации 95% атак);
- личный кабинет пользователя и экспорт отчета (в pdf формате);
- детектирование уязвимостей, аномалий и BotNet сетей как на момент их создания, так и функционирования на основе:
 - регулярных выражений;
 - поведенческого и эмпирического анализа;
 - отклонений от статистических показателей;
 - периодических проверок;
 - расширенная статистика подсчитывается как на основе "сырых" пакетов, так и взаимодействия NetFlow, BGP, SNMP; 100% контроль и мониторинг передаваемого трафика по сети; отображение статистики в реальном времени или за заданный промежуток с широкими возможностями фильтрации;
 - запрашиваемые хосты, URL, имена файлов и т.д.;

- подсчет тенденций и изменений популярности хостов и URL;
- выявление dns/http/ftp/prox/mail сервисов и анализ нагрузки на них;
- статистика по взаимодействию с соседними операторами;
- взаимодействие с оборудованием оператора: мониторинг загрузки интерфейсов, загруженность CPU, загруженность памяти, нестабильности маршрутов и т.д.;
- возможности по планированию расширения сети.

Встроенное решение СОРМ полностью соответствует техническим требованиям Минсвязи РФ, тем самым нет необходимости ставить дополнительное пассивное решение.

Аппаратно-программный комплекс автоматического обнаружения и блокирования DDOS-атак «АНТИ-DDOS»

Функциональность:

- фоновый статистический контроль метрик сети с целью обнаружения профиля злоумышленника;
- автоматическое блокирование трафика злоумышленника во всей контролируемой сети;
- настраиваемые уровни и режимы контроля для выделенных подсетей, личный кабинет для клиентов оператора;
- блокирование атак, исходящих от клиентов;
- специальные функции защиты от сильно распределенных атак;
- возможность ручного анализа и задания правил;
- возможность распределения сети зондов;
- возможность активной защиты WEB-сервисов на уровне прикладных сессий;
- детектирование широкого спектра DDoS-атак;
- отчеты в режиме реального времени;
- автоматическая запись дампов трафика атак, ретроспективный анализ.

Базовый список обнаруживаемых атак:

- сканирование информационно-телекоммуникационных ресурсов;

- нелегитимный трафик на невостребованный протокол и/или порт (UDP Flood, ICMP Flood);
- атака фрагментами IP-пакетов с некорректным содержимым;
- медленные DoS атаки, SlowLoris, SlowPost и их аналоги;
- инициация соединения на транспортном уровне стека TCP/IP (TCP Syn Flood);
- установка полноценного TCP-соединения с его дальнейшим сбрасыванием без обмена данными внутри socket (TCP Connection Flood);
- атака с использованием протокола DNS и генерацией легитимных запросов/ответов, в том числе DNS Amplification;
- атака с использованием протокола NTP и генерацией легитимных запросов/ответов, включая NTP-Amplification;
- отправка данных по протоколу HTTP/1.0 или HTTP/1.1 вне спецификации протокола;
- атака на SIP-сервис;
- атака на SMTP-сервис;
- атака на FTP-сервис;
- spoofing атаки любого уровня сложности, такие как TCP и UDP;
- широко распространенные атаки TCP, UDP (в том числе HTTP Flood);
- распределенная атака на специфический сервис Заказчика.

Технические характеристики:

- зонд 1RU с возможностью обработки до 10 Гбит/с транзитного трафика, включая различные варианты floods;
- возможность безопасного включения в разрыв канала либо в схему BGP маршрутизации;
- аппаратные средства включения с функцией отказоустойчивости;
- возможность аппаратной балансировки нагрузки с каналов 40 Гбит/с и 100 Гбит/с;
- комплекс предназначен для использования в ядре сети оператора связи / Интернет провайдера. Возможна интеграция услуг DDoS-защиты в спектр услуг оператора связи.

Контрольные вопросы:

1. Расскажите о методологии обеспечения информационной безопасности.
2. Перечислите и охарактеризуйте основные российские и международные стандарты в сфере обеспечения информационной безопасности.
3. Расскажите о стадиях (этапах и шагах) разработки и управления обеспечения информационной безопасности.
4. Проведите сравнение (по функциональным параметрам) продукции российской компании «Норси-Транс» с зарубежными техническими решениями по обеспечению информационной безопасности.

Список литературы

а) Основная литература

1. Остапенко Г.А., Мешкова Е.А. Информационные атаки и атаки в социотехнических системах: учебное пособие для высших учебных заведений /под редакцией В.Г. Кулакова. М.: Горячая линия - Телеком, 2008г. 208с.
2. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования. М.: Издательский центр «Академия», 2013. 336с.
3. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети. Сетевые аномалии: учебное пособие для вузов /под ред. проф. О.И. Шелухина. М.: Горячая линия – Телеком, 2013. 220с.
4. Проскурин В.Г. Защита программ и данных: учебное пособие для студ. учреждений высш. проф. образования, 2-е издание. М.: Издательский центр «Академия», 2012. 208с.
5. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие. СПб.: Питер, 2017. 256с.
6. Курило А.П, Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью: учебное пособие для вузов, 2-е издание, испр. М.: Горячая линия – Телеком, 2014. 244с. Серия «Вопросы управления информационной безопасностью. Выпуск 1».

7. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности: учебное пособие для вузов, 2-е издание, испр. М.: Горячая линия – Телеком, 2014. 130с. Серия «Вопросы управления информационной безопасностью. Выпуск 2».

8. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Проверка и оценка деятельности по управлению информационной безопасностью: учебное пособие для вузов, 2-е издание, испр. М.: Горячая линия – Телеком, 2014. 166с. Серия «Вопросы управления информационной безопасностью. Выпуск 5».

9. ГОСТ Р ИСО/МЭК 27005-2010.

10. ГОСТ Р ИСО/МЭК 27004-2011.

11. ГОСТ Р ИСО/МЭК 27003-2012.

12. ГОСТ Р 56545-2015.

13. ГОСТ Р 56546-2015.

14. ГОСТ Р 53113.1-2008.

15. ГОСТ Р 53113.2-2009.

б) Дополнительная литература

1. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2004. 616с.

2. С. Норкат, Д. Новак. Обнаружение нарушений безопасности в сетях: 3-е издание, пер. с англ. М.: Издательский дом «Вильямс», 2003. 448с.

3. Бабин С.А. Инструментарий Хакера. СПб.: БХВ-Петербург, 2015. 240с.

4. Касперски К. Записки исследователя компьютерных вирусов. СПб.: Питер, 2006. 316с.

5. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности: учебное пособие для высших учебных заведений. М.: Горячая линия - Телеком, 2012г. 140с.

6. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие для вузов, 2-е издание, испр. М.: Горячая линия – Телеком, 2014. 170с. Серия «Вопросы управления информационной безопасностью. Выпуск 3».

7. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие для вузов, 2-е издание, испр. М.: Горячая линия – Телеком, 2012. 214с. Серия «Вопросы управления информационной безопасностью. Выпуск 4».
8. Скобцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2017. 272 с.
9. Яковлев В.А. Шпионские и антишпионские штучки. СПб.: Наука и Техника, 2015. 320с.
10. Дудихин В.В., Дудихина О.В. Конкурентная разведка в Интернет: 2-е изд., испр. и доп. М.: Издательство «АСТ», 2004. 229 с.
11. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2017. 272 с.

в) Ресурсы сети «Интернет»

1. Электронная библиотека учебных материалов ЯрГУ: http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php.
2. Информационная система "Единое окно доступа к образовательным ресурсам" (<http://www.edu.ru> (раздел Учебно-методическая библиотека) или по прямой ссылке <http://window.edu.ru/library>).
3. Электронно-библиотечная система «Университетская библиотека online»: www.biblioclub.ru.
4. Новости в сфере угроз безопасности и защиты компьютерной информации российского журнала «Хакер» (<https://hacker.ru/tag/news>) и журнала «Информационная безопасность»(<http://itsec.ru/main.php>).
5. Новейшие данные об угрозах работы с подключением к сети Интернет российской компании «Лаборатория Касперского»: <http://www.kaspersky.ru/internet-security-center>.
6. Материалы ежегодного всемирного конгресса хакеров «Chaos Communication Congress» в Гамбурге (на английском языке), где рассказывается о новых методах компьютерной разведки и выявленных уязвимостях в аппаратных решениях и программном обеспечении: https://events.ccc.de/congress/2015/wiki/Static:Main_Page, видеоматериалы с субтитрами на нескольких языках конгресса CCC: <https://www.youtube.com/user/CCCEn/videos>.

Глоссарий использованных сокращений и терминов

Антихакинг – условный термин противодействия методам взлома систем безопасности.

Апгрейт – замена или улучшение программных, или аппаратных решений.

АС - автоматизированная система.

АСОД – автоматизированная система обработки данных.

АО - аппаратное обеспечение.

Вредоносная программа - программа, предназначенная для несанкционированного доступа и/или воздействия на информацию или ресурсы информационной системы.

ГИС – государственная информационная система.

ИБ - информационная безопасность.

ИС - информационная система.

ИОА - информационные операции и атаки.

ИТ - информационные технологии.

ИТТ – информационные телекоммуникационные технологии.

КИИ - критическая информационная инфраструктура, выведение которой из строя повлечет за собой тяжкие или критические последствия.

КР - компьютерная разведка, проводимая с помощью компьютерных телекоммуникационных средств и систем связи, в значительной степени компьютеризированных в настоящее время.

Криптоанализ - наука о раскрытии алгоритмов шифрования, подборе ключей и восстановлении информации из зашифрованного сообщения.

НДВ - недекларированные возможности.

НСД - несанкционированный доступ.

ОИБ – обеспечение (иногда - оценка) информационной безопасности.

ОО – объект оценки в информационной безопасности.

ПО - программное обеспечение.

ПолиИБ - Политика информационной безопасности.

РД - Руководящий документ.

СЗИ - средства защиты информации.

СК – скрытый информационный канал. Скрытый информационный канал - это предусмотренный разработчиком

системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

Снифферы - программы мониторинга и анализа сетевого трафика.

СОА - система обнаружения компьютерных сетевых атак.

СОВ – система обнаружения компьютерных вторжений в информационные системы и сети.

СОПКА – система обнаружения и противодействия компьютерным атакам.

СТС – социально-техническая информационная система или среда.

СУИБ - система управления информационной безопасностью.

СУНБ - системы управления национальной безопасностью.

ТК - телекоммуникационные компании.

ТКЭ - технико-криминалистическая экспертиза.

Эксплойт - («exploit», англ. - использовать в своих интересах, часто в смысле - злоупотреблять) это компьютерная программа, фрагмент программного кода или последовательность команд, использующая уязвимости в программном обеспечении (или заложенные разработчиками недокументированные функции обхода подсистемы безопасности) для проведения атаки на вычислительную систему.

Оглавление

Введение	3
1. Цели и задачи компьютерной разведки, формы и условия ее проведения. Роль, место и формы противодействия компьютерной разведке.....	6
1.1. Цели, задачи и особенности проведения компьютерной конкурентной разведки, использования методов компьютерной разведки в меркантильных противоправных целях, а также в противоправных политических целях для реализации идеологии терроризма и экстремизма	7
1.2. Роль, место и формы организационно-юридического и технического противодействия методам компьютерной разведки объектов российской информационной инфраструктуры	17
2. Методы выявления признаков и фактов проведения компьютерной разведки	24
2.1. Компьютерные атаки, основные понятия и определения, классификация атак, этапы реализации атак, основные механизмы реализации атак, реализация атак, завершение атаки	25
2.2. Выявление признаков и фактов проведения компьютерной разведки в широкополосных сетях, сетях общего доступа, современных беспроводных сетях связи, на отдельных критически важных объектах информационной инфраструктуры. Использование штатных общедоступных технологий мониторинга в качестве самостоятельных инструментов. Программы анализа и мониторинга сетевого трафика, обзор сниферов	36
2.3. Проверка устройств на возможное наличие закладных аппаратных или программных средств компьютерной разведки на критически важных объектах сетевой инфраструктуры России	45
3. Оценка уязвимости систем для компьютерной разведки.....	52
3.1. Выявление уязвимости объектов информатизации для средств проведения компьютерной разведки.....	52
3.2. Оценка эффективности принимаемых защитных мер.....	64

3.3. Дополнительный анализ истории и содержания инцидентов безопасности (по материалам аналитического отчета InfoWatch) .	67
4. Средства и методы обнаружения вторжений в информационные системы.....	77
4.1. Выявление и отражение компьютерных атак	78
4.2. «Антихакинг» как система выявления признаков злонамеренного изучения открытых сервисов и защитных механизмов системы. Правила безопасного использования Интернета и соцсетей	84
4.3. Системы обнаружения вторжений	92
5. Противодействие программным закладкам	102
5.1. Принципы построения политики безопасности, обеспечивающей высокую защищенность от программных закладок. Методы выявления программных закладок: сигнатурное и эвристическое сканирование. Мониторинг информационных потоков, антивирусные средства, изолированная программная среда.....	102
5.2. Контроль целостности программного обеспечения. Контроль целостности конфигурации защищаемой системы	112
5.3. Программные ловушки	117
5.4. Организационные и административные меры защиты от программных закладок.....	117
6. Комплекс мер технического противодействия компьютерной разведке	125
6.1. Разработка вариантов совершенствования имеющихся мер технического противодействия компьютерной разведке на российских объектах информатизации.....	126
6.2. Современные и перспективные российские аппаратные, программные и аппаратно-программные комплексы технического противодействия компьютерной разведке, их назначение и функциональные возможности.....	152
Список литературы.....	162
Глоссарий использованных сокращений и терминов	165
Оглавление	167

Учебное издание

Техническое противодействие компьютерной разведке

Часть 1

Учебно-методическое пособие

Составитель

Ушаков Юрий Игоревич

Редактор, корректор Н.А. Трубникова

Верстка Н.А. Трубникова

Подписано в печать 11.12.17. Формат 60×84 1/16.

Усл. печ. л. 9,82. Уч.-изд. л. 7,2.

Тираж 4 экз. Заказ

Ярославский государственный университет им. П. Г. Демидова
150003, Ярославль, ул. Советская, 14