Методы обеспечения непрерывности бизнеса

1. Введение

1.1. Ретроспектива проблемы опеспечения безопасности в инфокоммуникациях.

Исторически проблема опеспечения безопасности и обеспечения непрерывности фунционирования инфокоммуникационных систем в организации появилась в начале 50-х годов связана с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи безопасности решались способами ограничения физического доступа к оборудованию. Кроме того количество копьютеоров было ограниченным и они имели четко определенную специализацию. Количество людей разбирающихся в том как работает ЭВМ было тоже ограниченным и требовала огромного объема знаний и нескольких лет обучения.

На следующем этапе (начиная с 1975 года) создаются и развиваются локальные информационно-коммуникационные сети и появляются Персональные ЭВМ. Задачи обеспечения безопасности также решались способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам. Но именно в этот переод стали появлятся первые вирусы, которые в основном переносились на электронных носителях. Количество ЭВМ стало измерятся сотнями и хотя обучение все еще требовалось объем заний значительно снизился.

III этап-- начиная с 1995 года -- связан с использованием появлением с массовой опрационной системы Windows которая имела интутивно понятный интерфейс, освоение которго заниало пару недель. Также в этот время стал рапространятся интернет , пока еще не широкополосный, а с использование модемов. Иммено на это этапе родились множесво атак сетевых атак (Ping of Death, DDOS, SQL- Инъекции). Проблема обеспечения беопасности не была так остра но для некоторых организий она стала важной задачей.

IV этап -- начиная с 2010 года-- связан с созданием и развитием глобалной сети интернет и мобильных компьютеров (смартфонов). Теперь доступ к информации может происходит с любой точки мира где есть мобильная связь (3G, 4 G) или Wi-Fi. Интерфейс компьютеров упростился до такой стпени что даже ребенокможет начать использовать устройство после нескольких минут знакомства. Большинство процессов которе раньше происходили в бумажном виде теперь цифровизированы. Большинство процессов управления в организации тоже бзируются на цифровых коммуникациях. Поэтому проблема обеспечения инфокуммоникационной

безопасности встала в полный рост и касается не только организаций но и индивилумов. На этом этапе ущерб наностится матеиальному благосостоянию – кража средств с кредитных карт , незаконные переводы.

V- этап, который наступит в 2025 - 2030 связан с созданием роботизированных устройств, которые будут должны не просто помогать, но и обеспечивать безопасность (например автомобии под управлением автопилота) . В этом случае под угрозу поставлена не только материальные ценности но и жизнь человека.

Как можно заметить из перечисленных этапов проблема аоьеспечения безопасности и непрерывности работы бизнеса становится с каждым годом все важнее. В будущем интсруктаж по кибер безопасности станет такой же стандартоной и обязательной процедурой как обкчение пожароной безопасности или техники безопасности на рабочем месте.

1.2. Облачные вычисления

В первые идея того, что мы сегодня называем облачными вычислениями была озвучена J.C.R. Licklider, в 1970 году. В эти годы он был ответственным за создание ARPANET (Advanced Research Projects Agency Network). Его идея заключалась в том, что каждый человек на земле будет подключен к сети, из которой он будет получать не только данные на и программы. Другой ученый John McCarthy высказал идею о том, что вычислительные мощности будут предоставляться пользователям как услуга (сервис). На этом развитие облачных технологий было приостановлено до 90-х годов, после чего ее развитию поспособствовал ряд факторов.

1. Расширение пропускной способности Интернета, в 90-е годы не позволило получить значительного скачка в развитии в облачной технологии, так как практически ни одна компания не технологии того времени не были готовы к этому. Однако сам факт ускорения Интернета дал толчок скорейшему развитию облачных вычислений.

2. Одним из наиболее значимых событий в данной области было появление Salesforce.com в 1999 году. Данная компания стала первой компанией предоставившей доступ к своему приложению через сайт, по сути данная компания стала первой компанией предоставившей свое программное обеспечение по принципу – программное обеспечение как сервис (SaaS).

3. Следующим шагом стала разработка облачного веб-сервиса компанией Amazon в 2002 году. Данный сервис позволял хранить, информацию и производить вычисления.

4. В 2006, Amazon запустила сервис под названием Elastic Compute cloud (EC2), как веб-сервис который позволял его пользователям запускать свои собственные приложения. Сервисы Amazon EC2 и Amazon S3 стали первыми доступными сервисами облачных вычислений.

5. Другая веха в развитие облачных вычислений произошла после создания компанией Google, платформы Google Apps для веб-приложений в бизнес секторе.

6. Значительную роль в развитии облачных технологий сыграли технологии виртуализации, в частности программное обеспечение позволяющее создавать виртуальную инфраструктуру.

7. Развитие аппаратного обеспечения способствовало не столько быстрому росту облачных технологий, сколько доступности данной технологии для малого бизнеса и индивидуальных лиц. Что касается технического прогресса, то значительную роль в этом сыграло создание многоядерных процессоров и увеличения емкости накопителей информации.

Облачные вычисления в настоящее время.

Википедия дает следующее определение облачных вычислений. Облачные вычисления (англ. cloud computing) — технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис. Предоставление пользователю услуг как Интернет-сервис является ключевым. Однако под Интернет-сервисом не стоит понимать доступ к сервису только через Интернет, он может осуществляться также и через обычную локальную сеть с использованием веб-технологий.

Из определения и истории видно, что основой для создания и быстрого развития облачных вычислительных систем послужили крупные интернет сервисы, такие как Google, Amazon и др, а так же технический прогресс, что по сути говорит о том что появление облачных вычислений было всего лишь делом времени. Рассмотрим каким же образом развитие вышеперечисленных направлений позволило облачным системам стать доступнее.

1. Развитие многоядерных процессоров привело к:
   увеличению производительности, при тех же размерах оборудования;
   — снижение стоимости оборудования, как следствие эксплуатационных расходов;
   — снижение энергопотребления облачной системы, для большинства ЦОД это действительно проблема при наращивании мощностей ЦОД.
2. Увеличение емкостей носителей информации, снижение стоимости хранения 1 Мб информации позволило:
   — безгранично (по крайней мере так позиционируют себя большинство «облаков») увеличить объемы хранимой информации;
   — снизить стоимость обслуживания хранилищ информации, значительно увеличив объемы хранимых данных.
3. Развитие технологии многопоточного программирования привело к:
   — эффективному использованию вычислительных ресурсов многопроцессорных систем;
   — гибкое распределение вычислительных мощностей облаков.
4. Развитие технологий виртуализации привело к:

— созданию программного обеспечения позволяющего создавать виртуальную инфраструктуру не зависимо от количества предоставленных аппаратных ресурсов;
— легкость масштабирования, наращивания систем;
— уменьшение расходов на администрирование облачных систем;
— доступность виртуальной инфраструктуры через сеть Интернет.

5. Увеличении пропускной способности привело к:
— увеличению скорости работы с облачными системами в частности виртуальный графический интерфейс и работа с виртуальными носителями информации;
— снижение стоимости Интернет трафика для работы с большими объемами информации;
— проникновению облачных вычислений в массы.

Все вышеперечисленные факторы привели к повышению конкурентоспособности облачных вычислений в ИТ сфере.

Достоинства облачных вычислений

Доступность – облака доступны всем, из любой точки, где есть Интернет, с любого компьютера, где есть браузер. Это позволяет пользователям (предприятиям) экономить на закупке высокопроизводительных, дорогостоящих компьютеров. Также сотрудники компаний становятся более мобильными так, как могут получить доступ к своему рабочему месту из любой точки земного шара, используя ноутбук, нетбук, планшетник или смартфон. Нет необходимости в покупки лицензионного ПО, его настройки и обновлении, вы просто заходите на сервис и пользуетесь его услугами заплатив за фактическое использование.

Низкая стоимость – основные факторы снизившие стоимость использования облаков следующие:

— снижение расходов на обслуживания виртуальной инфраструктуры, вызванное развитием технологий виртуализации, за счет чего требуется меньший штат для обслуживания всей ИТ инфраструктуры предприятия;

— оплата фактического использования ресурсов, пользователь облака платит за фактическое использование вычислительных мощностей облака, что позволяет ему эффективно распределять свои денежные средства. Это позволяет пользователям (предприятиям) экономить на покупке лицензий к ПО;

— использование облака на правах аренды позволяет пользователям снизить расходы на закупку дорогостоящего оборудования, и сделать акцент на вложение денежных средств на наладку бизнес процессов предприятия, что в свою очередь позволяет легко начать бизнес;

— развитие аппаратной части вычислительных систем, в связи с чем снижение стоимости оборудования.

Гибкость — неограниченность вычислительных ресурсов (память, процессор, диски), за счет использования систем виртуализации, процесс

масштабирования и администрирования «облаков» становиться достаточно легкой задачей, так как «облако» самостоятельно может предоставить вам ресурсы, которые вам необходимы, а вы платите только за фактическое их использование.

надежность – надежность «облаков», особенно находящихся в специально оборудованных ЦОД, очень высокая так, как такие ЦОД имеют резервные источники питания, охрану, профессиональных работников, регулярное резервирование данных, высокую пропускную способность Интернет канала, высокая устойчивость к DDOS атакам.

безопасность – «облачные» сервисы имеют достаточно высокую безопасность при должном ее обеспечении, однако при халатном отношении эффект может быть полностью противоположным.

большие вычислительные мощности – вы как пользователь «облачной» системы можете использовать все ее вычислительные способности, заплатив только за фактическое время использования. Предприятия могут использовать данную возможность для анализа больших объемов данных.

Недостатки

постоянное соединение с сетью – для получения доступа к услугам «облака» необходимо постоянное соединение с сетью Интернет. Однако в наше время это не такой и большой недостаток особенно с приходом технологий сотовой связи 3G и 4G.

программное обеспечение и его кастомизация – есть ограничения по ПО которое можно разворачивать на «облаках» и предоставлять его пользователю. Пользователь ПО имеет ограничения в используемом ПО и иногда не имеет возможности настроить его под свои собственные цели.

Конфиденциальность – конфиденциальность данных хранимых на публичных «облаках» в настоящее вызывает много споров, но в большинстве случаев эксперты сходятся в том, что не рекомендуется хранить наиболее ценные для компании документы на публичном “облаке”, так как в настоящее время нет технологии которая бы гарантировала 100% конфиденциальность хранимых данных.

надежность – что касается надежности хранимой информации, то с уверенностью можно сказать что если вы потеряли информацию хранимую в “облаке”, то вы ее потеряли навсегда.

безопасность – “облако” само по себе является достаточно надежной системой, однако при проникновении на него злоумышленник получает доступ к огромному хранилищу данных. Еще один минус это использование систем виртуализации, в которых в качестве гипервизора используются ядра стандартные ОС такие, как Linux, Windows и др., что позволяет использовать вирусы.

дороговизна оборудования – для построения собственного облака компании необходимо выделить значительные материальные ресурсы, что не выгодно только что созданным и малым компаниям.

Виды услуг предоставляемые облачными системами

Что касается предоставляемых услуг, то в настоящее время концепция облачных вычислений предполагает оказание следующих типов услуг своим пользователям:

— все как услуга (Everything as a Service); При таком виде сервиса пользователю будет предоставлено все от программно аппаратной части и до управлением бизнес процессами, включая взаимодействие между пользователями, от пользователя требуется только наличие доступа в сеть Интернет. На мой взгляд, данный вид сервиса это более общее понятие по отношению к нижеприведенным услугам, являющимися более частными случаями.

— инфраструктура как услуга (Infrastructure as a service);Пользователю предоставляется компьютерная инфраструктура, обычно виртуальные платформы (компьютеры) связанные в сеть. Которые он самостоятельно настраивает под собственные цели.

— платформа как услуга (Platform as a service); Пользователю предоставляется компьютерная платформа, с установленной операционной системой возможно и с программным.

— программное обеспечение как услуга (Software as a service); Данный вид услуги обычно позиционируется как «программное обеспечение по требованию», это программное обеспечение развернутое на удаленных серверах и пользователь может получать к нему доступ посредством Интернета, причем все вопросы обновления и лицензий на данное программное обеспечение регулируется поставщиком данной услуги. Оплата в данном случае производиться за фактическое использование программного обеспечения.

— аппаратное обеспечение как услуга (Hardware as a Service); В данном случае пользователю услуги предоставляется оборудование, на правах аренды которое он может использовать для собственных целей. Данный вариант позволяет экономить на обслуживании данного оборудования, хотя по своей сути мало чем отличается от вида услуги «Инфраструктура как сервис» за исключением того что вы имеете голое оборудование на основе которого разворачиваете свою собственную инфраструктуру с использованием наиболее подходящего программного обеспечения.

— рабочее место как услуга (Workplace as a Service); В данном случае компания использует облачные вычисления для организации рабочих мест своих сотрудников, настроив и установив все необходимое программное обеспечение, необходимое для работы персонала.

— данные как услуга (Data as a Service); Основная идея данного вида услуги заключается в том, что пользователю предоставляется дисковое пространство, которое он может использовать для хранения больших объемов информации.

Классификация облачных сервисов.

В настоящее время выделяют три категории «облаков»:
1. Публичные;
2. Частные;
3. Гибридные.

Публичное облако — это ИТ-инфраструктура используемое одновременно множеством компаний и сервисов. Пользователи данных облаков не имеют возможности управлять и обслуживать данное облако, вся ответственность по этим вопросам возложена на владельца данного облака. Абонентом предлагаемых сервисов может стать любая компания и индивидуальный пользователь. Они предлагают легкий и доступный по цене способ развертывания веб-сайтов или бизнес-систем, с большими возможностями масштабирования, которые в других решениях были бы недоступны. Примеры: онлайн сервисы Amazon EC2 и Simple Storage Service (S3), Google Apps/Docs, Salesforce.com, Microsoft Office Web.

Частное облако — это безопасная ИТ-инфраструктура, контролируемая и эксплуатируемая в интересах одной-единственной организации. Организация может управлять частным облаком самостоятельно или поручить эту задачу внешнему подрядчику. Инфраструктура может размещаться либо в помещениях заказчика, либо у внешнего оператора, либо частично у заказчика и частично у оператора. Идеальный вариант частного облака это облако развернутое на территории организации, обслуживаемое и контролируемое ее сотрудниками.

Гибридное облако — это ИТ- инфраструктура использующая лучшие качества публичного и приватного облака, при решении поставленной задачи. Часто такой тип облаков используется, когда организация имеет сезонные периоды активности, другими словам, как только внутренняя ИТ-инфраструктура не справляется с текущими задачами, часть мощностей перебрасывается на публичное облако (например большие объемы статистической информации, которые в необработанном виде не представляют ценности для предприятия), а также для предоставления доступа пользователям к ресурсам предприятия (к частному облаку) через публичное облако.

Облачные технологии являются неотъемлемой частью современного ИТ ладшафта это необходимо учитывать как при анализе рисков так и при выборе метотодов защиты.Особенно для обеспечения непрерывности бизнеса в условиях ограниченности ресурсов.

1.3. Определение безопасности

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

· Конфиденциальность -- состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

· Целостность -- избежание несанкционированной модификации информации;

· Доступность -- избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

· Неотказуемость или апеллируемость -- невозможность отказа от авторства;

· Подотчётность -- обеспечение идентификации субъекта доступа и регистрации его действий;

Примеры угроз связяанных с доступностью

Угроза доступности (отказа служб) возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным - запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Доступность информации– свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда возникает в этом необходимость.

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибкиштатных пользователей, операторов, системных администраторов и других лиц, обслуживающих ИС.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники. По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе. Самый радикальный способ борьбы с непреднамеренными ошибками – максимальная автоматизация и строгий контроль.

Другие угрозы доступностиклассифицируем покомпонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;

- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой;
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

- отступление от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

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

Весьма опасны так называемые "обиженные" сотрудники – нынешние и бывшие (они стремятся нанести вред организации-"обидчику", например: испортить оборудование; встроить логическую бомбу, которая со временем разрушит программы и/или данные; удалить данные). Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствияи события, воспринимаемые как стихийные бедствия,– пожары, наводнения, землетрясения, ураганы, по статистике, (среди которых самый опасный – перебой электропитания) приходится 13% потерь, нанесенных ИС.

Некоторые примеры угроз доступности.

Угрозы доступности могут выглядеть грубо – как повреждениеили даже разрушениеоборудования(в том числе носителей данных) и может вызываться естественными причинами (чаще всего – грозами). Опасны протечки

водопровода и отопительной системы, в сильную жару, ломаются кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители обычно хранят небрежно, не обеспечивая их защиту от вредного воздействия окружающей среды.

Перейдем теперь к программным атакам на доступность.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов(обычно – полосы пропускания сетей, вычислительных возможностей процессоров или ОЗУ). По расположению источника угрозы такоепотреблениеподразделяется налокальное и удаленное. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов – атака, получившая наименование "SYN-наводнение". Она представляет собой попытку переполнить таблицу "полуоткрытых" TCP-соединений сервера (установление соединений начинается, но не заканчивается), что приводит к затруднению установление новых соединений пользователей, то есть сервер блокируется.

По отношению к атаке "Papa Smurf" уязвимы сети, воспринимающие ping-пакеты с широковещательными адресами. Ответы на такие пакеты "съедают" полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме – как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание.

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentium I дает возможность локальному пользователю путем выполнения определенной команды "подвесить" компьютер, так что помогает только аппаратный RESET.

Программа "Teardrop" удаленно "подвешивает" компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.

Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую, в том числе и несанкционированное изменение информации при случайных ошибках программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, периодическая запланированная коррекция некоторой базы данных).

Целостность информации - существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Обычно субъектов интересует обеспечение более широкого свойства –

достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т.е. ее неискаженности.

На втором месте по размерам ущерба стоят кражи иподлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. В наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, знакомые с режимом работы и мерами защиты, что подтверждает опасность внутренних угроз, хотя им уделяют меньшее внимание, чем внешним.

Существует различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник может:ввести неверные данные; изменить данные.

Иногда изменяются содержательные данные, иногда – служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее начальником президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что в указанное время он разговаривал по мобильному телефону, находясь вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние "файл против файла". Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарша знала пароль вице-президента, поскольку ей было поручено его менять), и иск был отвергнут...

Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить "неотказуемость", компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально уязвимы с точки зрения нарушения целостностине толькоданные, но и программы. Внедрение рассмотренного выше вредоносного ПО – пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин "утечка".

Конфиденциальность информации– субъективно определяемая (приписываемая) характеристика (свойство) информации, указывающая н необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий доступа к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты их законных интересов от других субъектов информационных отношений.

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной смене только усугубляют положение, заставляя применять несложные схемы чередования или стараться свести дело к двум-трем легко запоминаемым паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита. Угроза же состоит в том, что кто-то не откажется узнать секреты, которые сами просятся в руки. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна – получить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Еще один пример изменения, о котором часто забывают, – хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Перехват данных – очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические

средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют.

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие какмаскарад– выполнение действий под видом лица, обладающего полномочиями для доступа к данным

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример – нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

2.Классификация угроз, атак и защищяемой информации.

2.1. Источники и типы угроз

Моделирование и классификацию источников угроз и их проявлений, целесообразно проводить на основе анализа взаимодействия логической цепочки:

источник угрозы - уязвимость - угроза - ущерб (атака).

Под этими терминами будем понимать:

Источник угрозы - это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Угроза [Threat]- это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.

Уязвимость [Vulnerability]- это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта

информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

Ущерб (атака) - это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся уязвимости.

Как видно из определения, атака - это всегда пара "источник - уязвимость", реализующая угрозу и приводящая к ущербу. При этом, анализ последствий предполагает проведение анализа возможного ущерба и выбора методов парирования угроз безопасности информации.

Угроз безопасности информации не так уж и много. Угроза, как следует из определения, это опасность причинения ущерба, то есть в этом определении проявляется жесткая связь технических проблем с юридической категорией, каковой является "ущерб".

Ущерб

Проявления возможного ущерба могут быть различны:

- моральный и материальный ущерб деловой репутации организации;
- моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;
- материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;
- материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;
- материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;
- моральный и материальный ущерб от дезорганизации деятельности организации;
- материальный и моральный ущерб от нарушения международных отношений.

Ущерб может быть причинен каким-либо субъектом и в этом случае имеется на лицо правонарушение, а также явиться следствием независящим от субъекта проявлений (например, стихийных случаев или иных воздействий, таких как проявления техногенных свойств цивилизации). В первом случае налицо вина субъекта, которая определяет причиненный вред как состав преступления, совершенное по злому умыслу (умышленно, то есть деяние совершенное с прямым или косвенным умыслом) или по неосторожности (деяние, совершенное по легкомыслию, небрежности, в результате невиновного причинения вреда) и причиненный ущерб должен квалифицироваться как состав преступления, оговоренный уголовным правом.

Во втором случае ущерб носит вероятностный характер и должен быть сопоставлен, как минимум с тем риском, который оговаривается гражданским, административным или арбитражным правом, как предмет рассмотрения.

В теории права под ущербом понимается невыгодные для собственника имущественные последствия, возникшие в результате правонарушения. Ущерб выражается в уменьшении имущества, либо в недополучении дохода, который был бы получен при отсутствии правонарушения (упущенная выгода).

При рассмотрении в качестве субъекта, причинившего ущерб какую-либо личность, категория "ущерб" справедлива только в том случае, когда можно доказать, что он причинен, то есть деяния личности необходимо квалифицировать в терминах правовых актов, как состав преступления. Поэтому, при классификации угроз безопасности информации в этом случае целесообразно учитывать требования действующего уголовного права, определяющего состав преступления.

Вот некоторые примеры составов преступления, определяемых Уголовным Кодексом Российской Федерации.

Хищение - совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества.

Копирование компьютерной информации - повторение и устойчивое запечатление информации на машинном или ином носителе.

Уничтожение - внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводятся в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота.

Уничтожение компьютерной информации - стирание ее в памяти ЭВМ.

Повреждение - изменение свойств имущества при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования.

Модификация компьютерной информации - внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных.

Блокирование компьютерной информации - искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

Несанкционированное уничтожение, блокирование модификация, копирование информации - любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией.

Обман (отрицание подлинности, навязывание ложной информации) - умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений.

Однако, говорить о злом умысле личности в уничтожении информации в результате стихийных бедствий не приходится, как и тот факт, что вряд ли стихия сможет воспользоваться конфиденциальной информацией для извлечения собственной выгоды. Хотя и в том и в другом случае собственнику

информации причинен ущерб. Здесь правомочно применение категории "причинение вреда имуществу". При этом, речь пойдет не об уголовной ответственности за уничтожение или повреждение чужого имущества, а о случаях подпадающих под гражданское право в части возмещения причиненного ущерба (риск случайной гибели имущества - то есть риск возможного нанесения убытков в связи с гибелью или порчей имущества по причинам, не зависящим от субъектов). По общему правилу в этом случае убытки в связи с гибелью или порчей имущества несет собственник, однако, гражданское право предусматривает и другие варианты компенсации причиненного ущерба.

При рассмотрении в качестве субъекта, причинившего ущерб какое-либо природное или техногенное явление, под ущербом можно понимать невыгодные для собственника имущественные последствия, вызванные этими явлениями и которые могут быть компенсированы за счет средств третьей стороны (страхование рисков наступления события) или за счет собственных средств собственника информации.

Например, страхование представляет собой отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов. Объектами страхования могут быть не противоречащие законодательству Российской Федерации имущественные интересы связанные с возмещением страхователем причиненного им вреда личности или имуществу физического лица, а также вреда, причиненного юридическому лицу.

Классификация угроз информационной безопасности

Обобщая изложенное, можно утверждать, что угрозами безопасности информации являются:

- хищение (копирование) информации;
- уничтожение информации;
- модификация (искажение) информации;
- нарушение доступности (блокирование) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность) так и объективные проявления. Причем, источники угроз могут находиться как внутри защищаемой организации - внутренние источники, так и вне ее - внешние источники. Деление источников на субъективные и объективные оправдано исходя из предыдущих рассуждений по поводу вины или риска ущерба информации. А деление на внутренние и внешние источники оправдано потому, что для одной и той же угрозы методы парирования для внешних и внутренних источников могу быть разными.

Все источники угроз безопасности информации можно разделить на три основные группы:

- Обусловленные действиями субъекта (антропогенные источники угроз).
- Обусловленные техническими средствами (техногенные источники угрозы).
- Обусловленные стихийными источниками.

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорит о причинении ущерба. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты информации.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

- криминальные структуры;
- потенциальные преступники и хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков телематических услуг;
- представители надзорных организаций и аварийных служб;
- представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

- основной персонал (пользователи, программисты, разработчики);
- представители службы защиты информации;
- вспомогательный персонал (уборщики, охрана);
- технический персонал (жизнеобеспечение, эксплуатация).

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты, которые могут быть из числа

основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угрозам для этой группы могут иметь свои отличия.

Квалификация антропогенных источников информации играют важную роль в оценке их влияния и учитывается при ранжировании источников угроз.

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако, последствия, вызванные такой деятельностью вышли из под контроля человека и существуют сами по себе. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.

Технические средства, являющиеся источниками потенциальных угроз безопасности информации так же могут быть внешними:

- средства связи;
- сети инженерных коммуникации (водоснабжения, канализации);
- транспорт.

и внутренними:

- некачественные технические средства обработки информации;
- некачественные программные средства обработки информации;
- вспомогательные средства (охраны, сигнализации, телефонии);
- другие технические средства, применяемые в учреждении;

Третья группа источников угроз объединяет, обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз информационной безопасности как правило являются внешними по отношению к защищаемому объекту и под ними понимаются прежде всего природные катаклизмы:

- пожары;
- землетрясения;
- наводнения;

- ураганы;
- различные непредвиденные обстоятельства;
- необъяснимые явления;
- другие форс-мажорные обстоятельства.

Классификация уязвимостей безопасности

Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости (факторы), приводящие к нарушению безопасности информации на конкретном объекте информатизации.

Уязвимости присущи объекту информатизации, неотделимы от него и обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации) Кроме того, возможно не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Для удобства анализа, уязвимости разделены на классы (обозначаются заглавными буквами), группы (обозначаются римскими цифрами) и подгруппы (обозначаются строчными буквами). Уязвимости безопасности информации могут быть:

- объективными
- субъективными
- случайными.

Объективные уязвимости

Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации. К ним можно отнести:

- сопутствующие техническим средствам излучения
  - электромагнитные (побочные излучения элементов технических средств , кабельных линий технических средств , излучения на частотах работы генераторов , на частотах самовозбуждения усилителей)
  - электрические (наводки электромагнитных излучений на линии и проводники , просачивание сигналов в цепи

электропитания, в цепи заземления , неравномерность потребления тока электропитания)
        - звуковые (акустические , виброакустические)
    - активизируемые
        - аппаратные закладки (устанавливаемые в телефонные линии , в сети электропитания , в помещениях , в технических средствах)
        - программные закладки (вредоносные программы , технологические выходы из программ , нелегальные копии ПО)
    - определяемые особенностями элементов
        - элементы, обладающие электроакустическими преобразованиями (телефонные аппараты , громкоговорители и микрофоны , катушки индуктивности , дроссели , трансформаторы и пр.)
        - элементы, подверженные воздействию электромагнитного поля (магнитные носители , микросхемы , нелинейные элементы, поверженные ВЧ навязыванию)
    - определяемые особенностями защищаемого объекта
        - местоположением объекта (отсутствие контролируемой зоны , наличие прямой видимости объектов , удаленных и мобильных элементов объекта , вибрирующих отражающих поверхностей)
        - организацией каналов обмена информацией (использование радиоканалов , глобальных информационных сетей , арендуемых каналов)

Субъективные уязвимости

Субъективные уязвимости зависят от действий сотрудников и, в основном, устраняются организационными и программно-аппаратными методами:

- ошибки
    - при подготовке и использовании программного обеспечения (при разработке алгоритмов и программного обеспечения , инсталляции и загрузке программного обеспечения , эксплуатации программного обеспечения , вводе данных)
    - при управлении сложными системами (при использовании возможностей самообучения систем , настройке сервисов универсальных систем , организации управления потоками обмена информации)
    - при эксплуатации технических средств (при включении/выключении технических средств , использовании технических средств охраны , использовании средств обмена информацией)
- нарушения

- режима охраны и защиты (доступа на объект , доступа к техническим средствам)
- режима эксплуатации технических средств (энергообеспечения , жизнеобеспечения)
- режима использования информации (обработки и обмена информацией , хранения и уничтожения носителей информации , уничтожения производственных отходов и брака)
- режима конфиденциальности (сотрудниками в нерабочее время , уволенными сотрудниками).

Случайные уязвимости

Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам информационной безопасности:

- сбои и отказы
  - отказы и неисправности технических средств (обрабатывающих информацию , обеспечивающих работоспособность средств обработки информации , обеспечивающих охрану и контроль доступа)
  - старение и размагничивание носителей информации (дискет и съемных носителей , жестких дисков , элементов микросхем , кабелей и соединительных линий)
  - сбои программного обеспечения (операционных систем и СУБД , прикладных программ , сервисных программ , антивирусных программ)
  - сбои электроснабжения (оборудования, обрабатывающего информацию , обеспечивающего и вспомогательного оборудования)
- повреждения
  - жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации , кондиционирования и вентиляции)
  - ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий , корпусов технологического оборудования)

2.2. Этапы атаки

Атака - это совокупность действий злоумышленника, приводящих к нарушению информационной безопасности ИС. Результатом успешной атаки

может стать, например, несанкционированный доступ нарушителя к информации, хранящейся в ИС, потеря работоспособности системы или искажение данных в ИС. В качестве целей атаки могут рассматриваться серверы, рабочие станции пользователей или коммуникационное оборудование ИС. При организации информационных атак злоумышленники часто используют специализированное ПО, позволяющее автоматизировать действия, выполняемые на различных стадиях атаки. программный маршрутизация локальный сеть

В общем случае в любой атаке можно выделить четыре стадии

Сбор информации. На этой стадии нарушитель старается получить как можно больше информации об объекте атаки, чтобы на ее основе спланировать дальнейшие этапы вторжения. Этим целям может служить, например, информация о типе и версии ОС, установленной на хостах ИС; список пользователей, зарегистрированных в системе; сведения об используемом прикладном ПО и т. д.

Поиск уязвимостей. На этом этапе нарушитель определяет какие уязвимости могут быть использованы для получения доступа к ресурсам тех хостов, на которые совершается атака.

Атакующее воздействие. На данной стадии реализуются те цели, ради которых и предпринималась атака, - например, нарушение работоспособности ИС, кража конфиденциальной информации из системы, удаление или модификация данных и т. д. При этом атакующий часто выполняет операции, направленные на удаление следов его присутствия в ИС.

Развитие атаки. Злоумышленник стремится расширить объекты атаки, чтобы продолжить несанкционированные действия на других составляющих ИС.

Рассмотрим на конкретных примерах, как могут реализовываться эти стадии. Так, на этапе сбора информации действия нарушителя могут быть нацелены на получение следующих данных: о структуре и топологии ИС, о типе ОС, о типе прикладных сервисов, о зарегистрированных пользователях.

Для получения информации о структуре и топологии системы нарушитель может воспользоваться стандартными утилитами, такими, как traceroute, входящими в состав практически любой ОС, которые позволяют сформировать список IP-адресов транзитных маршрутизаторов вплоть до хоста-объекта нападения. Информацию о структуре ИС злоумышленник может получить и путем обращения к DNS-серверу.

Один из наиболее распространенных методов определения типа ОС основан на том, что различные системы по-разному реализуют требования RFC, определяющие правила взаимодействия с сетевыми протоколами. При одних и тех же сетевых запросах разные ОС отправляют в ответ разные данные, и по ним можно с большой долей вероятности определить характеристики атакуемой ОС и даже тип аппаратной платформы.

Информацию о типе прикладных сервисов нарушитель может получить путем сканирования открытых портов и анализа заголовков ответов, полученных от этих служб. Данные же о зарегистрированных пользователях

можно извлечь из базы данных SNMP MIB, установленной на рабочих станциях и серверах ИС.

Когда необходимая информация собрана, можно начинать поиск уязвимостей. Всякая атака основана на наличии в ИС уязвимостей, и "правильное" использование хотя бы одной из них открывает злоумышленнику вход в систему.

Примеров уязвимостей можно привести немало. Здесь и ошибки при конфигурировании сетевых служб ИС, и ошибки в ПО, не "закрытые" пакетами обновления (service packs, patches, hotfixes), и использование "слабых" и "нестойких" паролей, и отсутствие необходимых средств защиты, и многое другое. В результате же нарушитель получает несанкционированный доступ к ресурсам атакованного хоста, что позволяет ему перейти к следующей стадии информационной атаки.

На стадии атакующего воздействия нарушитель выполняет те действия, которые и составляют цель атаки, - например, извлекает из СУБД атакованного хоста номера кредитных карточек или другую конфиденциальную информацию.

После атакующего воздействия нарушитель может перевести атаку в фазу дальнейшего развития. Для этого в систему обычно внедряется программа, с помощью которой можно организовать атаку на другие хосты ИС. После ее установки опять начинается первый этап атаки - сбор информации о следующей цели.

2.3. Взлом паролей

Для взлома паролей используется не такой уж и широкий набор различных техник. Почти все они известны и почти любая компрометация конфиденциальной информации достигается за счет использования отдельных методов или их комбинаций.

Фишинг

Самый распространенный способ, которым на сегодняшний день «уводят» пароли популярных почтовых сервисов и социальных сетей — фишинг, и этот способ срабатывает для очень большого процента пользователей.

Суть метода в том, что пользователь попадает на, как ему кажется, знакомый сайт (тот же Gmail, ВК или Одноклассники, например), и по той или иной причине его просят ввести логин и пароль (для входа, подтверждения чего-либо, для его смены и т.п.). Сразу после ввода пароль оказывается у злоумышленников.

Как это происходит: пользователь может получить письмо, якобы от службы поддержки, в котором сообщается о необходимости войти в аккаунт и дана ссылка, при переходе на которую открывается сайт, в точности копирующий оригинальный. Возможен вариант, когда после случайной установки нежелательного ПО на компьютере, системные настройки изменяются таким образом, что при вводе в адресную строку браузера адреса

нужного вам сайта, пользователь на самом деле попадает на оформленный точно таким же образом фишинговый сайт.

При получении письма, которое в том или ином виде предлагает пользователю войти в его аккаунт на том или ином сайте, он должен обращатить внимание, действительно ли оно было отправлено с адреса почты на этом сайте: обычно используются похожие адреса. Например, вместо support@vk.com, может быть support@vk.org или нечто подобное. Однако, правильный адрес не всегда гарантирует, что все в порядке.

Подбор паролей

Атаки с использованием подбора паролей (Brute Force, грубая сила) также достаточно распространены. Если несколько лет назад большинство таких атак представляли собой действительно перебор всех комбинаций определенного набора символов для составления паролей определенной длины, то на данный момент всё обстоит несколько проще (для хакеров).

Анализ утекших за последние годы миллионов паролей показывает, что менее половины из них уникальны, при этом на тех сайтах, где «обитают» преимущественно неопытные пользователи, процент совсем мал.

Что это означает? В общем случае — то, что хакеру нет необходимости перебирать несчетные миллионы комбинаций: имея базу из 10-15 миллионов паролей (приблизительное число, но близкое к истине) и подставляя только эти комбинации, он может взломать почти половину аккаунтов на любом сайте.

В случае целенаправленной атаки на конкретную учетную запись, помимо базы может использоваться и простой перебор, а современное программное обеспечение позволяет это делать сравнительно быстро: пароль из 8-ми символов может быть взломан в считанные дни (а если эти символы представляют собой дату или сочетание имени и даты, что не редкость — за минуты).

Если пользователь использует один и тот же пароль для различных сайтов и сервисов, то как только его пароль и соответствующий адрес электронной почты будут скомпрометированы на любом из них, с помощью специального ПО это же сочетание логина и пароля будет опробовано на сотнях других сайтах.

Взлом сайтов и получение хэшей паролей

Большинство серьезных сайтов не хранят пароль в том виде, в котором его знает пользователь. В базе данных хранится лишь хэш — результат применения необратимой функции (то есть из этого результата нельзя снова получить ваш пароль) к паролю. При входе на сайт, заново вычисляется хэш и, если он совпадает с тем, что хранится в базе данных, значит пароль введен верно.

Как несложно догадаться, хранятся именно хэши, а не сами пароли как раз в целях безопасности — чтобы при потенциальном взломе и получении злоумышленником базы данных, он не мог воспользоваться информацией и узнать пароли.

Таблица 2.3.1. Результаты различных хэш функций.

Пароль	password
Хэш пароля, вычисленный по различным алгоритмам	
Adler32	0f910374
CRC32	35c246d5
Haval	2221b19499669a2da53c49caf3c5e5be
MD2	f03881a88c6e39135f0ecc60efd609b9
MD4	8a9d093f14f8701df17732b2bb182c74
MD5	5f4dcc3b5aa765d61d8327deb882cf99
RipeMD128	c9c6d316d6dc4d952a789fd4b8858ed7
RipeMD160	2c08e8f5884750a7b99f6f2f342fc638db25ff31
SHA-1	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
SHA-256	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd6
SHA-384	a8b64babd0aca91a59bdbb7761b421d4f2bb38280d3a75ba
SHA-512	b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b
Tiger	d476a6b8b5c35ce912781497d02d09faeb8aa05a489223f5
Whirlpool	5b59c49b6dc8bcb2a554a64c42e859c6d43c5fbfe9adc41d6

Однако, довольно часто, сделать это он может:

Для вычисления хэша используются определенные алгоритмы, в большинстве своем — известные и распространенные (т.е. каждый может их использовать).

Имея базы с миллионами паролей (из пункта про перебор), злоумышленник также имеет и доступ к хэшам этих паролей, вычисленным по всем доступным алгоритмам.

Сопоставляя информацию из полученной базы данных и хэши паролей из собственной базы, можно определить, какой алгоритм используется и узнать реальные пароли для части записей в базе путем простого сопоставления (для всех неуникальных). А средства перебора помогут узнать остальные уникальные, но короткие пароли.

Как видите, маркетинговые утверждения различных сервисов о том, что они не хранят пароли у себя на сайте, не обязательно защищают пользователей от их утечки.

Шпионские программы (SpyWare)

SpyWare или шпионские программы — широкий спектр вредоносного программного обеспечения, скрытно устанавливающегося на компьютер (также шпионские функции могут быть включены в состав какого-то нужного ПО) и выполняющего сбор информации о пользователе.

Помимо прочего, отдельные виды SpyWare, например, кейлоггеры (программы, отслеживающие нажимаемые вами клавиши) или скрытые анализаторы траффика, могут использоваться (и используются) для получения пользовательских паролей.

Социальная инженерия и вопросы для восстановления пароля

Социальная инженерия — метод доступа к информации, основанный на особенностях психологии человека (сюда можно отнести и упоминавшийся выше фишинг). В Интернете можно найти множество примеров использования социальной инженерии некоторые из которых поражают своей изящностью. В общих чертах метод сводится к тому, что почти любую информацию, необходимую для доступа к конфиденциальной информации, можно получить, используя слабости человека.

Приведем лишь простой бытовой пример, имеющий отношение к паролям. На многих сайтах для восстановления пароля достаточно ввести ответ на контрольный вопрос: в какой школе вы учились, девичья фамилия матери, кличка домашнего животного… Даже если пользователь уже не разместил эту информацию в открытом доступе в социальных сетях, не сложно с помощью тех же социальных сетей, будучи знакомым или специально познакомившись с ним, ненавязчиво получить такую информацию.

Атака с использованием словарей

При этом используется простой файл, содержащий слова, которые можно найти в словаре. Другими словами, атаки такого типа перебирают именно слова, которые многие люди используют в качестве пароля.

Такая "хитрость", как умело сгруппированные вместе слова, например, "симсимоткройся" или "ясуперадминистратор", не спасут пароль от взлома – возможно, хакеры всего лишь потратят несколько лишних секунд.

Атака методом полного перебора (грубой силы)

Этот метод похож на атаку по словарю, который позволяет обнаружить слова, не содержащиеся в словаре, перебирая все возможные буквенно-цифровые комбинации от aaa1 до zzz10.

Это не быстрый способ, особенно, если пароль состоит из нескольких символов, но, в конечном счете, пароль будет раскрыт. Метод полного перебора может быть упрощен с помощью использования дополнительных вычислительных мощностей компьютера, в том числе, с использованием возможностей видеокарты GPU - и, например, использования распределенных вычислительных моделей и ботнетов.

Атака с использованием радужной таблицы

Радужная таблица - это список предварительно вычисленных хэшей (числовых значений зашифрованных паролей), используемых большинством современных систем. Таблица включает в себя хэши всех возможных комбинаций паролей для любого вида алгоритма хэширования. Время, необходимое для взлома пароля с помощью радужной таблицы, сводится к тому времени, которое требуется, чтобы найти захэшированный пароль в списке. Тем не менее, сама таблица огромна и для просмотра требует серьезных вычислительных мощностей. Также она будет бесполезна, если хэш, который она пытается найти был усложнен добавлением случайных символов к паролю до применения алгоритма хеширования.

2.4. DDOS атаки

Distributed Denial of Service или «Распределенный отказ от обслуживания» — нападение на информационную систему для того, чтобы та не имела возможности обрабатывать пользовательские запросы. Простыми словами, DDoS заключается в подавлении веб-ресурса или сервера трафиком из огромного количества источников, что делает его недоступным. Часто такое нападение проводится, чтобы спровоцировать перебои в работе сетевых ресурсов в крупной фирме или государственной организации

DDoS-атака похожа на другую распространённую веб-угрозу — «Отказ в обслуживании» (Denial of Service, DoS). Единственное различие в том, что обычное распределенное нападение идет из одной точки, а DDos-атака более масштабна и идет из разных источников.

Основная цель DDoS-атаки — сделать веб-площадку недоступной для посетителей, заблокировав её работу. Но бывают случаи, когда подобные нападения производятся для того, чтобы отвлечь внимание от других вредных воздействий. DDoS-атака может, например, проводиться при взломе системы безопасности с целью завладеть базой данных организации.

DDoS-атаки появились в поле общественного внимания в 1999 году, когда произошла серия нападений на сайты крупных компаний (Yahoo, eBay, Amazon, CNN). С тех пор, этот вид кибер-преступности развился в угрозу глобального масштаба. По данным специалистов, за последние годы их частота возросла в 2,5 раза, а предельная мощность стала превышать 1 Тбит/сек. Жертвой DDoS-атаки хотя бы раз становилась каждая шестая российская компания. К 2020 году их общее число достигнет 17 миллионов

DDoS могут разрушить сайты любого масштаба, начиная от обычных блогов и заканчивая крупнейшими корпорациями, банками и другими финансовыми учреждениями.

Согласно исследованиям, проведенным «Лабораторией Касперского», нападение может стоить фирме до 1,6 млн долларов. Это серьезный урон, ведь атакованный веб-ресурс на какое-то время не может обслуживании, из-за чего происходит простой.

Чаще всего от DDoS-атак страдают сайты и сервера:

- крупных компаний и государственных учреждений;

- финансовых учреждений (банков, управляющих компаний);
- купонных сервисов;
- медицинских учреждений;
- платежных систем;
- СМИ и информационных агрегаторов;
- интернет-магазинов и предприятий электронной коммерции;
- онлайн-игр и игровых сервисов;
- бирж криптовалюты.

Не так давно к печальному списку частых жертв DDoS-атак добавилось и подключённое к интернету оборудование, получившее общее название «интернет вещей» (Internet of Things, IoT). Самую большую динамику роста на этом направлении показывают кибер-нападения с целью нарушить работу онлайн-касс больших магазинов или торговых центров.

Все веб-серверы имеют свои ограничения по числу запросов, которые они могут обрабатывать одновременно. Кроме этого, предусмотрен предел для пропускной способности канала, соединяющего Сеть и сервер. Чтобы обойти эти ограничения, ззлоумышленники создают компьютерную сеть с вредоносным программным обеспечением, называемую «ботнет» или «зомби-сеть».

Для создания ботнета кибер-преступники распространяют троян через e-mail рассылки, социальные сети или сайты. Компьютеры, входящие в ботнет не имеют физической связи между собой. Их объединяет только «служение» целям хозяина-хакера.

В ходе DDoS-атаки хакер отправляет команды «зараженным» компьютерам-зомби, а те начинают наступление. Ботнеты генерируют огромный объем трафика, способный перегрузить любую систему. Основными «объектами» для DDoS обычно становится пропускной канал сервера, DNS-сервер, а также само интернет-соединение.

Когда действия злоумышленников достигают своей цели, это моментально можно определить по сбоям в работе сервера или размещённого там ресурса. Но есть ряд косвенных признаков, по которым о DDoS-атаке можно узнать ещё в самом её начале.

Серверное ПО и ОС начинают часто и **явно сбоить** — зависать, некорректно завершать работу и т. д.

Резко возросшая **нагрузка на аппаратные мощности** сервера, резко отличающаяся от среднедневных показателей.

Стремительное увеличение **входящего трафика** в одном или ряде портов.

Многократно **дублированные однотипные действия** клиентов на одном ресурсе (переход на сайт, закачка файла).

При анализе логов (журналов действий пользователей) сервера, брандмауэра или сетевых устройств выявлено **много запросов** одного типа из разных источников **к одному** порту или сервису. Следует особо насторожиться, если аудитория запросов резко отличается от целевой для сайта или сервиса.

Классификация типов DDoS-атак

Протокольное наступление (транспортный уровень):

DDoS-атака направлена на сетевой уровень сервера или веб-ресурса, поэтому её часто называют атакой сетевого уровня или транспортного уровня. Её цель— привести к перегрузке табличного пространства на межсетевом экране со встроенным журналом безопасности (брандмауэре), в центральной сети или в системе, балансирующей нагрузку.

Самый распространённый метод DDoS на транспортном уровне — **сетевой флуд**, создание огромного потока запросов-пустышек на разных уровнях, с которыми физически не может справится принимающий узел.

Обычно сетевая служба применяет правило FIFO, согласно которому компьютер не переходит к обслуживанию второго запроса, пока не обработает первый. Но при атаке количество запросов настолько возрастает, что устройству недостает ресурсов для того, чтобы завершить работу с первым запросом. В итоге, флуд максимально насыщает полосу пропускания и наглухо забивает все каналы связи.

Распространённые виды сетевого флуда:

HTTP-флуд — на атакуемый сервер отправляется масса обычных или шифрованных HTTP-сообщений, забивающих узлы связи.

ICMP-флуд — ботнет злоумышленника перегружает хост-машину жертвы служебными запросами, на которые она обязана давать эхо-ответы. Частный пример такого типа атак — **Ping-флуд** или Smurf-атака, когда каналы связи заполняются ping-запросами, использующимися для проверки доступности сетевого узла. Именно из-за угрозы ICMP-флуда системные администраторы зачастую целиком блокируют возможность делать ICMP-запросы с помощью фаервола.

SYN-флуд — атака воздействует на один из базовых механизмов действия протокола TCP, известного как принцип «тройного рукопожатия» (алгоритм «запрос-ответ»: SYN пакет – SYN-ACK пакет – ACK пакет). Жертву заваливают валом фальшивых SYN-запросов без ответа. Канал пользователя забивается очередью TCP-подключений от исходящих соединений, ожидающих ответного ACK пакета.

UDP-флуд — случайные порты хост-машины жертвы заваливаются пакетами по протоколу UDP, ответы на которые перегружает сетевые ресурсы. Разновидность UDP-флуда, направленная на DNS-сервер, называется **DNS-флуд.**

MAC-флуд — целью являются сетевое оборудование, порты которого забиваются потоками «пустых» пакетов с разными MAC-адресами. Для защиты от подобного вида DdoS-атак на сетевых коммутаторах настраивают проверку валидности и фильтрацию MAC-адресов.

Атаки прикладного уровня (уровень инфраструктуры):

Эта разновидность используется, когда необходимо захватить или вывести из строя аппаратные ресурсы. Целью «рейдеров» может быть, как физическая, так и оперативная память или процессорное время.

Перегружать пропускной канал не обязательно. Достаточно только привести процессор жертвы к перегрузке или, другими словами, занять весь объем процессного времени.

Виды DDoS-атак прикладного уровня:

Отправка **«тяжелых» пакетов**, поступающие непосредственно к процессору. Устройство не может осилить сложные вычисления и начинает давать сбой, тем самым отключая посетителям доступ к сайту.

С помощью скрипта сервер наполняется **«мусорным» содержимым** — лог-файлами, «пользовательскими комментариями» и т.д. Если системный администратор не установил лимит на сервере, то хакер может создать огромные пакеты файлов, которые приведут к заполнению всего жесткого диска.

Проблемы с **системой квотирования.** Некоторые серверы используют для связи с внешними программами CGI-интерфейс (Common Gateway Interface, «общий интерфейс шлюза»). При получении доступа к CGI злоумышленник может написать свой скрипт, который станет использовать часть ресурсов, например — процессорное время, в его интересах.

Неполная проверка данных посетителя. Это также приводит к продолжительному или даже бесконечному использованию ресурсов процессора вплоть до их истощения.

Атака второго рода. Оно вызывает ложное срабатывание сигнала в системе защиты, что может автоматически закрыть ресурс от внешнего мира.

Атаки на уровне приложений:

DDoS-атака уровня приложений использует упущения при создании программного кода, которая создаёт уязвимость ПО для внешнего воздействия. К данному виду можно отнести такую распространённую атаку, как «Пинг смерти» (Ping of death) — массовая отправка компьютеру жертвы ICMP-пакетов большей длины, вызывающих переполнение буфера.

Но профессиональные хакеры редко прибегают к такому простейшему методу, как перегрузка пропускных каналов. Для атаки сложных систем крупных компаний, они стараются полностью разобраться в системной структуре сервера и написать эксплойт — программу, цепочку команд или часть программного кода, учитывающие уязвимость ПО жертвы и применяющиеся для наступления на компьютер.

DNS-атаки:

Первая группа направлена на **уязвимости в ПО** DNS-серверов. К ним относятся такие распространённые виды кибер-преступлений, как Zero–day attack («Атака нулевого дня») и Fast Flux DNS («Быстрый поток»). Один из самых распространённых типов DNS-атак называется DNS–Spoofing («DNS-спуфинг»). В ходе неё злоумышленники заменяют IP-адрес в кеше сервера, перенаправляя пользователя на подставную страничку. При переходе преступник получает доступ к персональным данным юзера и может использовать их в своих интересах. Например, в 2009 году из-за подмены DNS-записи пользователи не могли зайти в Twitter в течение часа. Такое нападение имело политический характер. Злоумышленники установили на главной

странице социальной сети предостережения хакеров из Ирана, связанные с американской агрессией

Вторая группа — это DdoS-атаки, которые приводят к **неработоспособности DNS-серверов**. В случае их выхода из строя пользователь не сможет зайти на нужную страницу, так как браузер не найдет IP-адрес, присущий конкретному сайту.

Предотвращение и защита от DDoS-атак

Согласно данным Corero Network Security, более ⅔ всех компаний в мире ежемесячно подвергаются атакам «отказа в доступе». Причём их число доходит до 50.

Владельцам сайтов, не предусмотревших защиту сервера от DDoS-атак, могут не только понести огромные убытками, но и снижением доверия клиентов, а также конкурентоспособности на рынке.

Самый эффективный способ защиты от DDoS-атак — фильтры, устанавливаемые провайдером на интернет-каналы с большой пропускной способностью. Они проводят последовательный анализ всего трафика и выявляют подозрительную сетевую активность или ошибки. Фильтры могут устанавливаться, как на уровне маршрутизаторов, так и с помощью специальных аппаратных устройств.

Способы защиты:

Применение брандмауэр для приложений — WAF (Web Application Firewall). Он просматривает переданный трафик и следит за легитимностью запросов.

Использование CDN (Content Delivery Network). Это сеть по доставке контента, функционирующая с помощью распределенной сети. Трафик сортируется по нескольким серверам, что снижает задержку при доступе посетителей.

Контролирование входящий трафик с помощью списков контроля доступа (ACL), где будут указан список лиц, имеющих доступ к объекту (программе, процессу или файлу), а также их роли.

Блокировка трафик, которых исходит от атакующих устройств. Делается это двумя методами: применение межсетевых экранов или списков ACL. В первом случае блокируется конкретный поток, но при этом экраны не могут отделить «положительный» трафик от «отрицательного». А во втором — фильтруются второстепенные протоколы. Поэтому он не принесет пользы, если хакер применяет первостепенные запросы.

Использование защиту от спам-ботов — капча (captcha), «человечные» временные рамки на заполнение форм, reCaptcha (галочка «Я не робот») и т. д.

Обратная атака. Весь вредоносный трафик перенаправляется на злоумышленника. Он поможет не только отразить нападение, но и разрушить сервер атакующего.

Размещение ресурсов на нескольких независимых серверах. При выходе одного сервера из строя, оставшиеся обеспечат работоспособность.

2.5. Ботнет

Ботнет — это сеть компьютеров, которые управляются хакерами удаленно.

Ботнеты используются преступниками для распространения программ-вымогателей на ваш ноутбук, телефон, планшет, компьютер. Они могут быть не обнаружены даже антивирусом, и вы можете долгое время не догадываться, что ваше устройство является частью ботнета.

Рис. 2.5.1. Структура ботнета.

Классическое понимание: слово «ботнет» представляет собой сочетание двух слов «робот» и «сеть». Здесь киберпреступник, выполняющий роль ботмастера, использует троянские вирусы, чтобы нарушить безопасность нескольких компьютеров и подключить их к сети в злонамеренных целях. Каждый компьютер в сети действует как «бот» и управляется мошенником для передачи вредоносных программ, спама или вредоносного контента для запуска атаки. Ботнет порой называют «армией зомби», т.к. компьютеры контролируются кем-то иным, кроме их владельца. Происхождение ботнетов главным образом зародилось в каналах интернет-чатов (IRC).

В конце концов, спамеры стали использовать уязвимости, присутствующие в сетях IRC, и разработали ботов.

Это было сделано специально для выполнения злонамеренных действий, таких как регистрация, эмуляция действий «заинтересованного клиента», кража

пароля и многое другое. Структура ботнета обычно принимает одну из двух форм: модель «клиент-сервер» или одноранговую модель (P2P, «Peer-to-peer»). Модель «клиент-сервер»

В структуре бот-системы «клиент-сервер», создается базовая сеть, в которой один сервер выступает в роли ботмастера. Ботмастер контролирует передачу информации от каждого клиента для установки команд и управления над клиентскими устройствами.

Модель «клиент-сервер» работает с помощью специального программного обеспечения и позволяет ботмастеру сохранять постоянный контроль над зараженными устройствами.

Эта модель имеет несколько недостатков: ее можно легко обнаружить, и она имеет только одну контрольную точку. В этой модели, если сервер уничтожен, ботнет погибает.

Рис. 2.5.2. Модель ботнета: клиент-сервер.

Чтобы преодолеть недостаток использования одного централизованного сервера, были созданы ботнеты современного типа. Они взаимосвязаны в форме одноранговой структуры.

В модели бот-сети P2P каждое подключенное устройство работает независимо как клиент и как сервер, координируя между собой обновление и передачу информации между ними.

Структура бот-сети P2P сильнее из-за отсутствия единого централизованного управления.

Рис. 2.5.2. Модель ботнета: клиент-сервер.

Распределенный отказ в обслуживании

Ботнет может использоваться для атаки распределенного отказа в обслуживании (DDoS) с целью уничтожения сетевых подключений и сервисов. Это делается путем перегрузки вычислительных ресурсов. Наиболее часто применяемыми атаками, являются атаки TCP SYN и UDP.

DDoS-атаки не ограничиваются только веб-серверами, но могут быть направлены на любую службу, подключенную к Интернету. Серьезность атаки может быть увеличена путем использования рекурсивных HTTP-потоков на веб-сайте жертвы, что означает, что боты рекурсивно следуют по всем ссылкам в HTTP-пути.

Эта форма называется «паутиной», и практикуется для более эффективного увеличения нагрузки.

Одна из крупнейших DDoS-атак ботнета 2018 года была связана с IoT и использовала вирус ботнета Mirai. Вирус предназначался для десятков тысяч менее защищенных интернет-устройств и контролировал их, превращая в ботов для запуска DDoS-атаки. Mirai породил множество производных запросов и продолжил расширяться, делая атаку более сложной. Это навсегда изменило ландшафт угроз с точки зрения используемых методов.

Спам и мониторинг трафика

Ботов можно использовать в качестве анализатора для выявления наличия конфиденциальных данных на зараженных машинах или компьютерах-зомби. Они также могут найти бот-сети конкурента (если они установлены на той же машине), и могут быть своевременно взломаны. Некоторые боты предлагают открыть прокси-сервер SOCKS v4 / v5 (универсальный протокол прокси для сети на основе TCP / IP). Когда прокси-сервер SOCKS включен на скомпрометированной машине, его можно использовать для различных целей,

например, для рассылки спама. Боты используют анализатор пакетов для отслеживания информации или данных, переданных скомпрометированной машиной. Сниффер может получить конфиденциальную информацию, такую как имя пользователя и пароль.

Keylogging

С помощью кейлоггера ботмастеру легко получить конфиденциальную информацию и украсть данные пользователя. Используя программу кейлоггер, злоумышленник может собрать только те ключи, которые набраны в последовательности клюевых слов, таких как PayPal, Yahoo и другое. Разновидность шпионского ПО, идентифицируемая как OSX / XSLCmd, перенесенная из Windows в OS X, включает в себя возможность ведения блогов и захвата экрана.

Массовая кража личных данных

Различные виды ботов могут взаимодействовать для совершения крупномасштабной кражи личных данных, что является одним из наиболее быстро растущих преступлений. С помощью ботов можно маскироваться под известный бренд и просить пользователя предоставить личные данные, такие как пароль банковского счета, данные кредитной карты, данные о налогообложении.

Массовая кража личных данных может быть осуществлена с использованием фишинговых писем, которые вынуждают жертв вводить учетные данные для входа на веб-сайты, как eBay, Amazon или даже известные коммерческие банки.

Злоупотребление платой за клик

Программа Google Ads позволяет веб-сайтам показывать рекламные объявления Google и тем самым зарабатывать на них деньги. Google платит деньги владельцам веб-сайтов на основании количества кликов, полученных от рекламы. Скомпрометированные машины используются для автоматического нажатия на ссылки, увеличивая количество фейковых кликов.

Adware

Рекламное программное обеспечение используется для привлечения пользователей за счет рекламы на веб-страницах или в приложениях. Они появляются на компьютерах без ведома или разрешения пользователей, а оригинальная реклама заменяется мошенническим рекламным ПО, которое заражает систему любых пользователей, кто на нее нажимает.

Рекламное программное обеспечение выглядит как безвредная реклама, но использует шпионское ПО для сбора данных браузера.

2.6. Классификация защищаемой информации

Государственная тайна

Государственная тайна — это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативнорозыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Сведения могут считаться государственной тайной (могут быть засекречены), если: - они соответствуют перечню сведений, составляющих государственную тайну, входят в перечень сведений, подлежащих засекречиванию, и отвечают законодательству Российской Федерации о государственной тайне (принцип законности); - целесообразность засекречивания конкретных сведений установлена путем экспертной оценки вероятных экономических и иных последствий, возможности нанесения ущерба безопасности Российской Федерации исходя из баланса жизненно важных интересов государства, общества и личности (принцип обоснованности); - ограничения на распространение этих сведений и на доступ к ним установлены с момента их получения (разработки) или заблаговременно (принцип своевременности); - компетентные органы и их должностные лица приняли в отношении конкретных сведений решение об отнесении их к государственной тайне и засекречиванию и установили в отношении них соответствующий режим правовой охраны и защиты (принцип обязательной защиты).

Конфиденциальная информация:

- Персональные данные;
- Тайна следствия, судопроизводства;
- Служебная тайна;
- Профессиональная тайна;
- Коммерческая тайна;
- Интеллектуальная собственность;

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Служебная тайна – защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основания и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости; На документах (в необходимых случаях и на их проектах) содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования»

Профессиональная тайна – информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности;

Виды профессиональной тайны: банковская, врачебная, адвокатская, нотариальная, аудиторская, таможенная, журналистская, налоговая, тайна связи, тайна страхования;

Примеры:

Банковская тайна. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте;

Врачебная тайна. Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений. ФЗ номер 5487-1 от 22.07.1993. «Основы законодательства РФ. Об охране здоровья граждан»;

Адвокатская, нотариальная тайна. Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. Нотариус обязан хранить в тайне сведения, которые стали ему известны в связи с осуществлением его профессиональной деятельности.

Журналистская тайна. Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне. Редакция обязана сохранить в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в производстве делом. Редакция не вправе разглашать в распространяемых сообщениях и материала сведения, прямо или косвенно указывающие на личность несовершеннолетнего, совершившего преступление либо подозреваемого в его совершении, а равно совершившего административное правонарушение или антиобщественное действие, без согласия самого несовершеннолетнего и его законного представителя.

Тайна связи. На территории РФ гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи; Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных Федеральными законами; Операторы связи обязаны обеспечить соблюдение тайны связи; Осмотр почтовых отправлений лицами, не являющимися уполномоченными работниками оператора связи, вскрытие почтовых отправлений, осмотр вложений, ознакомление с информацией и документальной корреспонденцией. Передаваемыми по сетям электросвязи Сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправления и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могу выдаваться только отправителям и получателям или их уполномоченным.

Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду; Информация, составляющая коммерческую тайну, - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа .

Интеллектуальная собственность ФЗ №230 от 18 декабря 2006 года «Гражданский кодекс РФ (часть 4)», ст.1225; Результатом интеллектуальной деятельности и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальной собственностью), являются: Произведения науки, литературы и искусства; Программы для ЭВМ; Базы данных; Исполнения; Фонограммы; Промышленные образцы; Селекционные достижения; Технологии интегральных микросхем; Секреты производства (ноу-хау); Фирменные наименования и т.д.;

Классификация защищаемой информации имеет важное значение, т.к. в дальнейшем для каждого из видов информации разрабатываются свои способы защиты. Вполне очевидно, что защита персональных данных, коммерческой, служебной и государственной тайны осуществляется различными способами, несмотря на то, что по содержанию эти сведения могут быть очень схожими. Например, сведения о банковских вкладах для сотрудников банка являются профессиональной (банковской) тайной, для организаций и предприятий — коммерческой тайной, а сведения о гражданах, являющихся вкладчиками, — их персональными данными. Если же подобные сведения предоставляются правоохранительным органам, то они приобретают статус служебной тайны, а если их приобретение стало результатом проведения оперативно-розыскных мероприятий, то такая информация является государственной тайной. В каждом из этих случаев применяются различные способы защиты информации.

3. Риск. Политика информационной безопасности.

3.1. Понятие риска

Прежде всего необходимо максимально полно и точно определить понятие риска. В BS 7799-3 дается наиболее широкое определение риска как комбинации вероятности события и его последствий. В отличие от спекулятивных рисков, когда событие может носить как позитивный характер (например, выигрыш в казино или на бирже), так и негативный (например, проигрыш), события информационной безопасности всегда носят негативный характер. Это позволяет отнести риски информационной безопасности к категории неспекулятивных рисков.

ISO 27005 конкретизирует понятие информационного риска, раскладывая его на активы, угрозы, уязвимости и ущерб. Согласно ISO 27005: «Риск информационной безопасности – это потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации».

Различные определения понятия «информационный риск»:

Риск – комбинация вероятности события и его последствий (BS 7799-3:2006).

Риск информационной безопасности – потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации (ISO/IEC 27005:2008).

Риск – неопределенность, предполагающая возможность потерь (ущерба) (СТО БР ИББС).

Риск – потенциальная проблема.

Риск – вероятные потери организации в результате инцидентов.

Понятие риска, данное в ISO 27005, пожалуй, является наиболее полным. Однако можно оперировать и более простыми и легко запоминающимися определениями. Например, риск можно рассматривать просто как потенциальную проблему либо как вероятные потери организации в результате инцидентов. В стандарте Банка России СТО БР ИББС риск определяется как «неопределенность, предполагающая возможность потерь».

Таким образом, риск является комплексной величиной, всегда определяемой через комбинацию ряда других величин. Это обусловливает ошибки в определении и описании конкретных рисков, нередко допускаемые даже специалистами, что вызывает трудности при оценке рисков.

Описание факторов риска, таких как угрозы, инциденты, уязвимости и виды ущерба, по отдельности не является описанием риска. О риске можно говорить только в том случае, если все факторы риска рассматриваются в совокупности. Только комбинация оценочных значений для угроз, уязвимостей и ущерба позволяет получить оценку риска.

Так, вопреки рекламным заявлениям некоторых разработчиков средств защиты информации, сетевые сканеры безопасности, прочие средства анализа защищенности информационных систем, так же как и средства контроля соответствия требованиям, включая средства анализа расхождений (gap analysis), не являются средствами оценки или управления рисками. Такие продукты лишь позволяют выявлять и анализировать определенные категории технических и организационных уязвимостей, а также в ряде случаев

идентифицировать определенные классы информационных активов, что, безусловно, является важной частью процесса оценки рисков, который, однако, включает в себя, помимо этого, еще много других элементов.

3.2. Оценка риска

Оценка риска заключается в определении его уровня (качественной либо количественной величины) и сравнении этого уровня с максимально допустимым (приемлемым) уровнем, а также с уровнем других рисков.

Уровень риска определяется путем комбинирования двух величин: вероятности события и размеров его последствий. Событие заключается в реализации угрозы, использующей уязвимости актива для воздействия на этот актив и нарушения его безопасности.

Под безопасностью информационного актива понимаются такие свойства информации, как конфиденциальность (защита от несанкционированного ознакомления), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения) и доступность (возможность за приемлемое время получить требуемую информационную услугу). Для упрощения дальнейшего изложения будем рассматривать только эту классическую триаду информационной безопасности, хотя к информационной безопасности относят также, по крайней мере, еще аутентичность (возможность подтверждения подлинности и достоверности документов) и неотказуемость (невозможность отрицания совершенных действий применительно к информационным активам).

Дополнительные «измерения» информационной безопасности необходимы для установления подотчетности (accountability) пользователей за действия, совершаемые ими в информационных системах. Например, некоторые злоумышленные или ошибочные действия, совершаемые в финансовой сфере, могут быть непосредственно не связаны с нарушением конфиденциальности, целостности или доступности какой-либо информации. Пользователь системы либо банковский служащий может перевести деньги с одного счета на другой, в последующем заявив о своей непричастности к данному деянию. Безопасность каких-либо информационных активов в данном случае не нарушается, при этом одной из сторон наносится прямой финансовый ущерб посредством манипулирования с информационными активами и системами. Для избежания подобных ситуаций и нужна подотчетность.

Нарушение безопасности актива обычно наносит ущерб организации. Величина этого ущерба определяет ценность актива для организации.

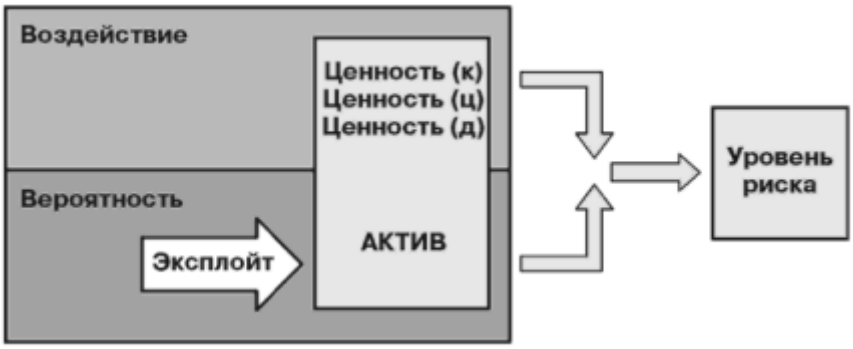

Рис. 3.2.1. Модель риска.

Оценка риска включает идентификацию и оценку ценности активов, последствий для бизнеса, идентификацию и оценку угроз и уязвимостей, а также комбинирование этих факторов для определения уровня риска в количественных и качественных величина

Количественное определение величины риска

Количественно величину риска, связанного с осуществлением конкретной угрозы безопасности в отношении конкретного актива, можно выразить при помощи следующей простой математической формулы:

.**[Величина риска] = [Вероятность события] × [Размер ущерба],**

где:

[Вероятность события] = [Вероятность угрозы] × [Величина уязвимости].

В этих формулах:

Вероятность события - Вероятность успешной реализации угрозы в отношении актива с использованием уязвимости и причинения ущерба организации

Вероятность угрозы - Вероятность того, что угроза в отношении актива будет реализовываться (успешность либо неуспешность реализации угрозы определяется величиной уязвимости). На практике для вычисления риска используется не математическая вероятность угрозы, а ожидаемое количество попыток реализации угрозы за определенный период времени. Специально, чтобы не было путаницы в стандартах, вместо математического термина probability используется понятие likelihood. Этот термин, хотя и переводится на русский так же, как «вероятность», на практике означает возможность реализации угрозы, характеризующуюся примерной частотой ее реализации за определенный период времени

Величина уязвимости - Вероятность того, что в случае реализации угрозы в отношении актива эта угроза будет реализована успешно с использованием данной уязвимости, т.е. безопасность актива в результате будет нарушена и организация понесет определенный ущерб

Для определения величины риска используются оценочные количественные значения, полученные путем экспертных оценок, прогнозирования, а также на основании статистических данных. Размер ущерба как правило выражается в денежных единицах, величина уязвимости принимает значения в диапазоне от 0 до 1, а вероятность угрозы является целым положительным числом, определяющим ожидаемое количество попыток реализации угрозы за определенный период времени.

Количественное определение величины риска:

[Величина риска] = [Вероятность угрозы]× [Величина уязвимости] × [Размер ущерба].

Для вычисления рисков удобно использовать период времени, равный одному году. В этом случае величина риска соответствует прогнозируемым среднегодовым потерям организации в результате инцидентов безопасности (Annual Loss Expectancy – ALE). Эту величину удобно использовать для соотнесения расходов на безопасность с величиной риска и для оценки возврата инвестиций, достигаемого за счет уменьшения величины риска, что соответствует определенному сокращению среднегодовых потерь организации.

Величина риска = Среднегодовые потери организации в результате осуществления угрозы в отношении актива с использованием уязвимости (ALE – Annual Loss Expectancy).

Это наиболее прагматичный и повсеместно используемый способ определения величины рисков. Потери организации выражаются в определенном денежном эквиваленте, ведь деньги – это наиболее универсальный инструмент для измерения ценности, применяемый в современном обществе. Каким бы ни был ущерб, материальный или нематериальный, прямой или косвенный, желательно его сопоставить определенной денежной величине. Иначе, что это за ущерб такой, ежели он ломаного гроша не стоит?

На практике оценка рисков всегда проводится на определенном уровне детализации. Все составляющие риска могут быть разложены на более мелкие составные элементы, что позволяет получить более точные и детализированные оценки рисков, и, наоборот, факторы риска могут быть сгруппированы для получения более общих оценок.

Поэтому формула для вычисления риска принимает следующий вид:

[Величина группы рисков] = [Ожидаемое количество попыток реализации группы угроз в течение года] × [Суммарная величина группы уязвимостей] × [Размер суммарного ущерба].

Практичная формула для определения величина рисков:

[Величина группы рисков] = [Ожидаемое количество попыток реализации группы угроз в течение года] × [Суммарная величина группы уязвимостей] × [Размер суммарного ущерба].

В зависимости от уровня детализации для одной организации могут рассматриваться от нескольких десятков до нескольких сотен и даже тысяч рисков информационной безопасности. Всегда следует начинать с высокоуровневой оценки рисков, которой соответствует наиболее низкий

уровень детализации, повышая детализацию по мере необходимости. Поводом для проведения более низкоуровневой (более детализированной) оценки рисков может служить то, что проведенная высокоуровневая оценка не предоставляет достаточной информации для принятия руководством организации обоснованных решений по обработке рисков.

Качественное определение величины риска

Конечно, точно определить вероятность угрозы, величину уязвимости либо размер ущерба на практике обычно не представляется возможным, поэтому речь может идти только о числовых оценках в некотором диапазоне величин. Так, оценочные среднегодовые потери (ALE) могут лежать в диапазоне от 100 тыс. до 1 млн. рублей, либо в диапазоне от 100 млн. рублей до 500 млн. рублей, либо превышать 1 млрд. рублей. Каждому количественному диапазону можно сопоставить определенный качественный уровень риска. В результате приходим к качественной шкале оценки риска, которой сопоставляются некоторые приблизительные количественные оценки, без которых любая качественная шкала лишается смысла, т.к. перестает быть связанной с реальными потерями организации.

На рис 3.2.2. приведен пример матрицы для определения величины риска. Такая матрица возникает в результате рассмотрения вероятности сценария инцидента с учетом влияния на бизнес. В этой матрице по горизонтали откладываются качественные значения вероятности успешной реализации угрозы (сценария инцидента), а по вертикали – качественные уровни ущерба (влияния на бизнес). Результирующий риск измеряется по шкале от 0 до 8, который может оцениваться по критериям принятия рисков, т.е. сравниваться с максимально допустимым уровнем риска, в качестве которого может быть выбрано, например, значение 3. Минимальный уровень риска, равный 0, соответствует очень низкой вероятности инцидента и очень низкому влиянию этого инцидента на бизнес, а максимальный уровень риска, равный 8, соответствует очень высокой вероятности инцидента и очень высокому влиянию на бизнес. Данная шкала рисков также может быть сведена к простому общему рейтингу риска, например: низкий риск: 0–2, средний риск: 3–5, высокий риск: 6–8. Все риски, значение которых превышает 3, будут нуждаться в обработке.

	Вероятность сценария инцидента	Очень низкая (очень маловероятно)	Низкая (маловероятно)	Средняя (возможно)	Высокая (вероятно)	Очень высокая (часто)
Влияние на бизнес	Очень низкое	0	1	2	3	4
	Низкое	1	2	3	4	5
	Среднее	2	3	4	5	6
	Высокое	3	4	5	6	7
	Очень высокое	4	5	6	7	8

Рис. 3.2.2. Матрица риска.

Вероятность сценария инцидента в свою очередь может быть представлена вероятностью осуществления угрозы и уровнем уязвимости. Комбинируя угрозу и уязвимости, которые используются для ее реализации, мы получаем сценарий инцидента.

Для определения значения вероятности инцидента может использоваться следующая матрица см рис. Рис. 3.2.3.

Вероятность угрозы	Низкая			Средняя			Высокая		
Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Значение вероятности сценария инцидента	0	1	2	1	2	3	2	3	4

Рис. 3.2.3. Матрица вероятности инцидента.

После определения уровня (величины) рисков, их необходимо проранжировать с целью определения приоритетов обработки этих рисков. Следующая таблица может использоваться для связи факторов ущерба (ценность актива) и вероятности инцидента (угроза и уязвимость объединяются и становятся причиной конкретного инцидента). На первом шаге по предопределенной шкале оценивается ущерб, например от 1 до 5 по каждому активу (столбец b в табл. 3.2.1). На втором шаге по предопределенной шкале оценивается вероятность осуществления инцидента, например, от 1 до 5 по каждому инциденту (столбец с в табл. 3.2.1). На следующем шаге вычисляется величина риска путем умножения b на с. В конечном итоге инциденты могут быть проранжированы по степени их критичности. Следует отметить, что в этом примере за 1 был принят самый низкий ущерб и самая низкая вероятность.

Таблица 3.2.1. Матрица ранжирующая инциденты по величине риска.

Дескриптор инцидента (a)	Ущерб (стоимость ресурса) (b)	Вероятность осуществления (c)	Величина риска (d)	Категория инцидента (e)
Инцидент A	5	2	10	2
Инцидент B	2	4	8	3
Инцидент C	3	5	15	1
Инцидент D	1	3	3	5
Инцидент E	4	1	4	4
Инцидент F	2	4	8	3

Приведенные выше способы качественного определения уровня риска и ранжирования инцидентов по уровню риска служат примерами табличных методов оценки рисков. Выбор конкретного табличного метода и настройка соответствующих шкал является прерогативой конкретной организации.

Еще раз подчеркнем, что любому качественному уровню, выражаемому числовыми значениями либо словами «низкий», «средний», «высокий» и т.п., должны соответствовать определенные диапазоны оценочных количественных величин. Без такого сопоставления использование качественных шкал для оценки рисков, конечно, возможно, однако в этом случае оценка рисков утрачивает экономический смысл.

Поэтому на практике количественный подход всегда превращается в качественный и наоборот, в связи с чем противопоставление качественных и количественных методов оценки рисков является, вообще говоря, занятием довольно бессмысленным.

Процесс сопоставления качественным уровням рисков соответствующих количественных диапазонов прогнозируемого среднегодового ущерба организации будет рассмотрен далее в соответствующей главе.

Информационная составляющая бизнес-рисков

Организации подвержены различным типам рисков, которые неизбежно сопровождают любую деятельность. Мы называем такие риски бизнес-рисками. Бизнес-риски отличаются большим разнообразием. Они могут быть классифицированы различными способами. Один из возможных подходов заключается в том, чтобы рассматривать источник риска. Примерами таких рисков являются инвестиционный, юридический, политический или рыночный риски. При другом подходе рассматривается природа актива, подвергающегося риску, примерами являются люди, имущество или информация. Еще один подход рассматривает последствия риска с точки зрения его долгосрочного, среднесрочного либо краткосрочного влияния на деятельность организации; примерами являются стратегический, тактический и операционный риски.

Категории бизнес-рисков:

- финансовые;
- политические;
- экономические;
- физические;
- юридические;
- стратегические;
- операционные;
- информационные;
- инвестиционные.

Риски информационной безопасности (информационные риски) – риски, которым подвергаются информационные активы организации. Информационные риски должны рассматриваться в качестве одной из основных категорий бизнес-риска. В зависимости от используемой классификации они могут быть отнесены к другим категориям, таким как стратегические и операционные риски. Система управления рисками информационной безопасности имеет дело со всеми информационными рисками, независимо от способа классификации.

Информационная составляющая есть во многих категориях рисков. Надо уметь выделять эту составляющую в любых бизнес-рисках. В следующей таблице приведены примеры угроз информационной безопасности, обуславливающих различные категории рисков, а также возможные последствия этих угроз.

Таблица 3.2.2 Примеры угроз информационной безопасности, обуславливающих различные категории рисков

Категория риска	Информационные угрозы	Последствия
Юридические (санкции со стороны регулирующих и правоохранительных органов)	Неисполнение требований законодательства и нормативной базы в области защиты информации Отсутствие необходимых лицензий Ошибки в договорах или налоговой отчетности	Штрафы, испорченная репутация, запрещение деятельности, выход из бизнеса
Рыночные (изменение ситуации на рынке, дефолты, девальвации и т.п.)	Несвоевременное получение информации Ошибки в прогнозах Фальсификация финансовой отчетности	Финансовые потери, потеря бизнеса

Инвестиционные (неправильные решения по вложению средств)	Недостаточная либо ложная информация, используемая для принятия инвестиционных решений Несвоевременное получение информации	Финансовые потери
Финансовые (ошибки учета, планирования, неправильное управление финансовыми активами, кража наличности, финансовое мошенничество и т.п.)	Финансовые махинации инсайдеров с использованием компьютерных систем Кибератаки на банковские счета Кибермошенничество с пластиковыми картами Фальсификация финансовой отчетности	Финансовые потери, ущерб репутации
Репутационные (негативные воздействия на имидж и репутацию компании)	Утечка конфиденциальной информации Невыполнение обязательств по причине недоступности информационных сервисов	Сокращение клиентской базы
Природные катаклизмы (Пожары, наводнения, землетрясения и т.п.)	Утрата информационных носителей и находящейся на них критичной для бизнеса информации Недоступность информационных сервисов	Финансовые потери, дезорганизация деятельности, потеря бизнеса
Техногенные (сбои оборудования или ПО)	Потеря критичной для бизнеса информации Потеря результатов работы	Финансовые потери, дезорганизация деятельности, невозможность исполнения обязательств
Физические (кража, ограбление, саботаж и т.п.)	Потеря критичной для бизнеса информации Утечка конфиденциальной информации Недоступность информационных сервисов	Ущерб репутации, финансовые потери, дезорганизация деятельности

Активы организации как ключевые факторы риска

Ключевым элементом риска является актив, подверженный этому риску. Риски информационной безопасности обусловлены наличием у организации информационных активов. К информационным активам относится любая информация, представляющая ценность для организации. Они включают в себя информацию, напечатанную или записанную на бумаге, пересылаемую по почте или демонстрируемую в видеозаписях, передаваемую устно, информацию, хранимую в электронном виде на серверах, веб-сайтах, мобильных устройствах, магнитных и оптических носителях и т.п., информацию, обрабатываемую в корпоративных информационных системах и передаваемую по каналам связи, а также программное обеспечение: операционные системы, приложения, утилиты, программную документацию и т.п.

Рис. 3.2.4. Группировка активов.

Помимо информации организация располагает и другими видами материальных и нематериальных активов, которые она использует для достижения своих бизнес-целей. Это имущество организации, имущественные и неимущественные права, интеллектуальная собственность, кадровые ресурсы, а также имидж и репутация организации. Современные международные стандарты также определяют еще одну категорию активов – это процессы, а также информационные и неинформационные сервисы. Это агрегированные типы активов, которые оперируют другими активами для достижения бизнес-целей.

Виды активов организации

- материальные;
- финансовые;
- имущественные и неимущественные права;
- интеллектуальная собственность;
- кадровые;
- информационные;
- процессы и сервисы;

- имидж и репутация.

Все активы определенным образом взаимосвязаны. Реализация угроз в отношении одних активов, например помещений или оборудования, может приводить к нарушению безопасности других активов, например информации, хранимой в этих помещениях или обрабатываемой на данном оборудовании, и т.д. В свою очередь нарушение безопасности информации, например ее конфиденциальности или достоверности, может обуславливать финансовые или политические риски. Сбой сервера влияет на доступность хранящихся на нем информации и приложений, а его ремонт отвлекает людские ресурсы, создавая их дефицит на определенном участке работ и вызывая дезорганизацию бизнес-процессов, при этом временная недоступность клиентских сервисов может негативно повлиять на имидж компании.

Таким образом, во многих видах бизнес-рисков есть информационная составляющая, обусловленная тем, что все активы организации и соответствующие риски в отношении этих активов связаны между собой.

Рассмотрим, например, физические угрозы, такие как пожар или землетрясение. С этими угрозами связаны, прежде всего, риски для жизни и здоровья людей, также с ними связаны риски потери оборудования и помещений, нарушения бизнес-операций, а также риски потери информационных активов, которые размещаются на этом оборудовании и в этих помещениях. Мы видим, что с одной и той же угрозой связано множество активов и уязвимостей, т.е. множество различных рисков, которые находятся в сфере компетенции различных людей: работников службы безопасности, пожарников, кадровиков, IT-специалистов, специалистов по управлению непрерывностью бизнеса.

Поэтому руководству организации, вообще говоря, было бы проще рассматривать все эти взаимосвязанные бизнес-риски в совокупности, в рамках единого процесса и общей методологии, охватывающей все виды информационных, физических и операционных рисков.

Все виды активов важны для организации. Однако у каждой организации есть основные активы и есть вспомогательные. Определить, какой актив является основным и жизненно важным, очень просто, т.к. бизнес организации построен вокруг основного актива. Так, бизнес может быть построен на владении и использовании материальных активов (земля, недвижимость, оборудование, полезные ископаемые), бизнес может быть построен на управлении финансовыми активами (кредитные организации, страхование, инвестирование), бизнес может быть основан на компетенции и авторитете конкретных специалистов (консалтинг, аудит, обучение, высокотехнологичные и наукоемкие отрасли) или все может вращаться вокруг информационных активов (разработка ПО, информационных продуктов, электронная коммерция, бизнес в Интернет).

Риски основных активов чреваты потерей бизнеса и невосполнимыми потерями, поэтому на этих рисках в первую очередь сосредоточено внимание

владельцев бизнеса и ими руководство организации занимается лично и в первую очередь. Риски вспомогательных активов приводят к восполнимому ущербу и не являются основным приоритетом в системе управления организации. Обычно управлением такими рисками занимаются специально назначаемые люди, либо эти риски передаются, скажем, аутсорсинговой организации. Управление такими неосновными рисками – это вопрос эффективности управления, а не выживания для организации.

Подходы к управлению рисками

Поскольку риски информационной безопасности являются основными далеко не для всех организаций, условно можно выделить три основных подхода к управлению этими рисками, различающиеся глубиной и уровнем формализма.

Различие подходов к управлению рисками:

Некритичные системы – применяется набор базовых требований безопасности, определяемых опытом, законодательством и стандартами.

Критичные системы – высокоуровневая оценка рисков. Особое внимание на системы с наибольшим риском.

Особо критичные системы – детальная оценка рисков с использованием формализованного подхода.

Для некритичных систем, когда информационные активы являются вспомогательными, а уровень информатизации невысок, что характерно для большинства современных российских компаний, существует минимальная необходимость в оценке рисков. В таких организациях следует вести речь о некотором базовом уровне ИБ, определяемом существующими нормативами и стандартами, лучшими практиками, опытом, а также тем, как это делается в большинстве других организаций. Однако существующие стандарты, описывая некоторый базовый набор требований и механизмов безопасности, всегда оговаривают необходимость оценки рисков и экономической целесообразности применения тех или иных механизмов контроля для того, чтобы выбрать из общего набора требования и механизмов те их них, которые применимы в конкретной организации. Поэтому определенные элементы оценки информационных рисков требуются и для таких организаций.

Для критичных систем, в которых информационные активы не являются основными, однако уровень информатизации бизнес-процессов очень высок и информационные риски могут существенно повлиять на основные бизнес-процессы, оценку рисков применять необходимо, но в данном случае целесообразно ограничиться неформальными качественными подходами к решению этой задачи, уделяя особое внимание наиболее критичным системам.

Когда бизнес построен вокруг информационных активов и риски информационной безопасности являются основными, необходимо применять формальный подход и проводить детализированную оценку рисков по всем активам.

Во многих компаниях одновременно несколько видов активов могут являться жизненно важными, например, когда бизнес диверсифицирован или компания занимается созданием информационных продуктов и для нее могут быть одинаково важны и людские и информационные активы. В этом случае рациональный подход заключается в проведении высокоуровневой оценки рисков, с целью определения того, какие системы подвержены рискам в высокой степени и какие имеют критическое значение для ведения деловых операций, с последующим проведением детальной оценки рисков для выделенных систем. Для всех остальных некритичных систем целесообразно ограничиться применением базового подхода, принимая решения по управлению рисками на основании существующего опыта, экспертных заключений и лучшей практики.

Заметим, что со временем доля критичных и особо критичных информационных систем в организациях любой сферы деятельности неуклонном повышается.

Таблица 3.2.3 Примеры организаций с высоким уровнем информационных рисков

Интернет-магазины, электронные биржи, расчетные системы, электронные торговые площадки	Основной акцент – киберугрозы и действия инсайдеров.
Производственные предприятия, использующие АСУТП	Основной акцент: физические, техногенные и киберугрозы, защита коммерческой и государственной тайны.
Телекоммуникационные компании	Основной акцент – непрерывность предоставления услуг. Риски: техногенные, антропогенные, физические, киберугрозы.
Банки, финансовые институты	Основной акцент – защита финансовых транзакций, предотвращение утечки информации и действий инсайдеров.

Учет каждого информационного актива (группы активов).

Риски должны оцениваться для каждого информационного актива, а не только для отдельных процессов или информационных систем.

Результаты оценки должны быть воспроизводимыми. Выводы должны быть аргументированы таким образом, чтобы независимые эксперты, используя те же методы, могли бы получить аналогичные результаты.

Руководство организации должно принимать риски осознанно. Другими словами, руководство должно осознавать реальные размеры и вероятность ущерба. Это достигается путем применения качественных и количественных

шкал оценки риска и их калибровки в соответствии с правилами, описанными ниже.

Обязательные элементы, которые должны быть отражены в выбранном организацией подходе к оценке рисков:

- определение критериев принятия риска;
- идентификация приемлемых уровней риска;
- идентификация и оценка рисков;
- охват всех аспектов области действия СУИБ, всех активов и областей контроля;
- учет каждого информационного актива (группы активов);
- воспроизводимость результатов;
- осознанное принятие рисков руководством организации.

Выбор подходов к оценке рисков определяется характером бизнеса организации и уровнем его информатизации, т.е. важностью для него информационных активов. Однако эффективность процесса управления рисками определяется не только точностью и полнотой анализа факторов риска и выбранным подходом, но также в значительной степени эффективностью механизмов принятия управленческих решений и контроля их исполнения, что целиком находится в компетенции высшего руководства организации.

Уровни зрелости бизнеса в отношении рисков

На выбор подхода к оценке рисков в организации, помимо характера ее бизнеса и уровня информатизации бизнес-процессов, также оказывает влияние ее уровень зрелости. Управление рисками – это бизнес-задача, инициируемая руководством организации в силу своей информированности и степени осознания проблем, смысл которой заключается в защите бизнеса от реально существующих угроз.

По степени осознания можно условно выделить несколько уровней зрелости организаций:

На первом уровне осознание как таковое отсутствует, в организации предпринимаются фрагментарные меры по обеспечению ИБ, инициируемые и реализуемые ИТ специалистами на свой страх и риск.

На втором уровне в организации определена ответственность за ИБ, делаются попытки применения интегрированных решений с централизованным управлением и внедрения отдельных процессов управления ИБ.

Третий уровень характеризуется применением процессного подхода к управлению ИБ, описанного в стандартах. Система управления ИБ становится настолько значимой для организации, что рассматривается как необходимый составной элемент системы управления организацией. Однако полноценной системы управления ИБ еще не существует, т.к. отсутствует базовый элемент этой системы – процессы управления рисками.

Для организаций с наивысшей степенью осознания проблем ИБ характерно применение формализованного подхода к управлению рисками ИБ, отличающегося наличием документированных процессов планирования, реализации, мониторинга и совершенствования СУИР.

Анализ факторов риска

Сущность любого подхода к управлению рисками заключается в анализе факторов риска и принятии адекватных решений по обработке рисков. Факторы риска – это те основные параметры, которыми мы оперируем при оценке рисков:

- актив (Asset);
- ущерб (Loss);
- угроза (Threat);
- уязвимость (Vulnerability);
- механизм контроля (Control);
- размер среднегодовых потерь (ALE);
- возврат инвестиций (ROI).

Способы анализа и оценки этих параметров определяются используемой в организации методологией оценки рисков. При этом общий подход и схема рассуждений примерно одинаковы, какая бы методология не использовалась.

Процесс оценки рисков (assessment) включает в себя две фазы.

На первой фазе, которая определяется в стандартах как анализ рисков (analysis), необходимо ответить на следующие вопросы:

- Что является активом компании?
- Какова реальная ценность данного актива?
- Какие существуют угрозы в отношении данного актива?
- Каковы последствия этих угроз и ущерб для бизнеса?
- Насколько вероятны эти угрозы?
- Насколько уязвим бизнес в отношении этих угроз?
- Каков ожидаемый размер среднегодовых потерь?

На второй фазе, которая определяется стандартами как оценивание рисков (evaluation), когда величина риска уже определена, необходимо ответить на вопрос: какой уровень риска (размер среднегодовых потерь) является приемлемым для организации и какие риски превышают этот уровень.

Таким образом, по результатам оценки рисков, включающей в себя процессы анализа и оценивания рисков, мы получаем описание рисков, превышающих допустимый уровень, и оценку величины этих рисков, которая определяется размером среднегодовых потерь. На выходе данного процесса формируется реестр информационных рисков, подробно рассматриваемый ниже.

Далее необходимо принять решение по обработке рисков, т.е. ответить на следующие вопросы:

Какой вариант обработки риска выбираем?

Если принимается решение об уменьшении риска, то какие механизмы контроля необходимо использовать?

Насколько эффективны эти механизмы контроля и какой возврат инвестиций они обеспечат?

На выходе данного процесса появляется план обработки рисков, определяющий способы обработки рисков, стоимость контрмер, а также сроки и ответственных за их реализацию.

Обзор методов оценки риска

В этом разделе в соответствии с международным стандартом ISO 31010 описываются 39 методов оценки риска, из которых 31 метод стандартизирован, а 8 - реально применяются на практике.

Международный стандарт ISO/IEC 31010 определяет следующие общие (не только для ИБ) методы оценки риска (эти методы можно комбинировать и применять на разных этапах оценки: идентификация риска, анализ угроз и последствий, определение уровня риска, оценивание риска):

- Мозговой штурм
- Структурированные или частично структурированные интервью
- Метод Дельфи
- Контрольные листы
- Предварительный анализ опасностей (PHA)
- Исследование опасности и работоспособности (HAZOP)
- Анализ опасности и критических контрольных точек (HACCP)
- Оценка токсикологического риска
- Структурированный анализ сценариев методом "Что, если?" (SWIFT)
- Анализ сценариев
- Анализ воздействия на бизнес (BIA)
- Анализ первопричины (RCA)
- Анализ видов и последствий отказов (FMEA)
- Анализ дерева неисправностей (FTA)
- Анализ дерева событий (ETA)
- Анализ причин и последствий
- Причинно-следственный анализ
- Анализ уровней защиты (LOPA)
- Анализ дерева решений
- Анализ влияния человеческого фактора (HRA)
- Анализ "галстук-бабочка"
- Техническое обслуживание, направленное на обеспечение надежности
- Анализ скрытых дефектов (SA)
- Марковский анализ
- Моделирование методом Монте-Карло
- Байесовский анализ и сети Байеса
- Кривые FN
- Индексы риска
- Матрица последствий и вероятностей
- Анализ эффективности затрат (CBA)
- Мультикритериальный анализ решений (MCDA)

Отметим, что на практике чаще применяются следующие не описанные в стандартах методы оценки риска:

- Метод отрицания необходимости и/или возможности оценки риска
- Метод отрицания наличия риска
- Метод интуитивной оценки риска
- Метод интуитивного принятия решений
- Метод голосования
- Метод голословных утверждений
- Метод общих рассуждений
- Моделирование угроз (российский метод)

Преимуществом данной группы методов является то, что они нересурсоемкие (за исключением моделирования нетиповых угроз) и самодостаточные (не требуют комбинирования с другими методами).

3.3 Обработка рисков

Оценка рисков позволяет получить ответы на три важнейших вопроса, а именно – какие информационные активы, от чего и зачем следует защищать. После этого успешность организации будет зависеть от того, какие меры она будет применять для обработки выявленных рисков. Основной вопрос руководителей: «Что делать?». Для того чтобы с этим вопросом разобраться, потребуется рассмотреть способы обработки рисков, а также подходы к оценке возврата инвестиций в безопасность и принятию остаточных рисков. Результатом этих усилий являются два ключевых документа, о которых пойдет речь далее: Декларация о применимости механизмов контроля и План обработки рисков.

Процесс обработки рисков

Целью обработки рисков является их уменьшение до приемлемого уровня путем уменьшения вероятности инцидента либо минимизации возможного ущерба. Однако не все риски возможно либо целесообразно уменьшать. Если организация не располагает необходимыми для этого ресурсами, например временем или квалификацией, то она может временно допустить высокий риск либо передать его третьей стороне путем заключения договора страхования или аутсорсинга. Возможен также вариант избежания риска путем отказа от рискованных операций либо переноса этих операций в более безопасное место.

Процесс обработки рисков включает в себя подготовку, выбор и принятие решений по способам обработки рисков. Способы эти могут быть самыми разными. Главное, чтобы они были реализуемы и экономически оправданы. При инвестировании денег в уменьшение риска в результате должен получаться положительный возврат инвестиций, который представляет собой разницу между затратами на безопасность и величиной предотвращаемого

ущерба. Разница эта должна быть весьма существенной. Желательно, чтобы возврат инвестиций превышал затраты на безопасность в разы.

На вход этого процесса поступают результаты оценки рисков в виде отчета и прилагающегося к нему реестра информационных рисков. Если эти данные являются достаточными, тогда для каждой группы рисков принимаются решения по их обработке путем выбора одного из четырех способов обработки рисков либо их комбинации. При этом используются критерии принятия рисков, определяемые политикой организации в области управления рисками.

Результатом процесса обработки рисков является план обработки рисков, содержащий перечни мероприятий для каждой группы рисков и оценку остаточных рисков.

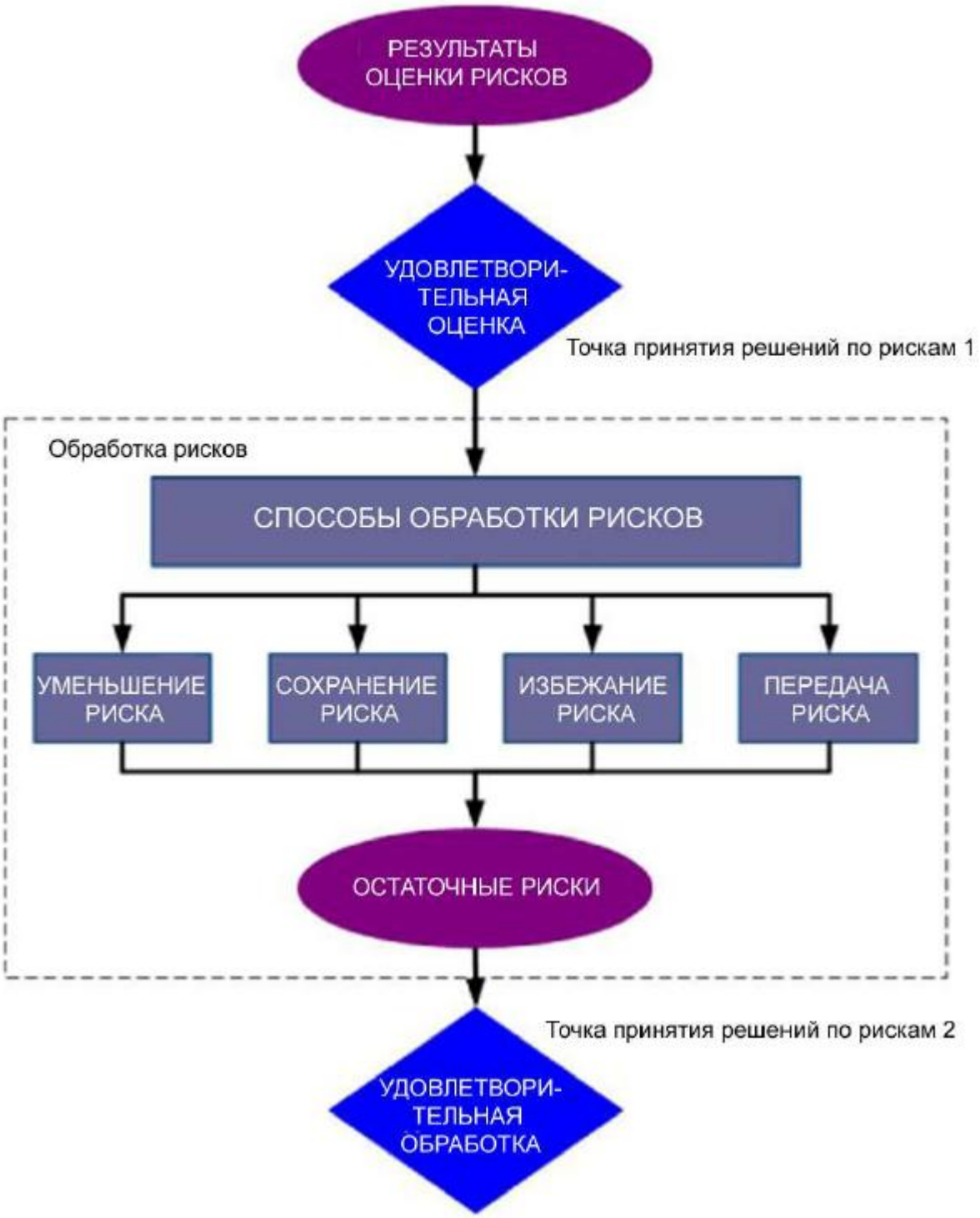

Рис. 3.3.1. Процесс обработки рисков.

Выбираемые для уменьшения рисков механизмы контроля должны быть экономически обоснованы, т.е. обеспечивать положительный возврат инвестиций. Однако не все механизмы контроля можно легко экономически обосновать. Например, обеспечение непрерывности бизнеса вынуждено иметь дело с такими рисками, как природные и антропогенные катастрофы, которые с большой вероятностью могут вообще никогда не наступить. Для механизмов обеспечения непрерывности бизнеса сложно посчитать возврат инвестиций, т.к. зачастую не существует оценки среднегодовых потерь.

Способы обработки рисков не являются взаимоисключающими. Например, мы можем уменьшить риск до определенного уровня, а остаточных риск передать третьей стороне.

Определенные способы обработки рисков могут воздействовать сразу на группу рисков, – например, такой множественный эффект дает обучение.

В ходе обработки рисков могут быть сделаны выводы в том числе и об избыточности некоторых механизмов контроля. Однако, прежде чем от них оказываться, следует оценить их влияние на другие механизмы. Многие механизмы контроля взаимосвязаны. Эффективность одних механизмов может снижаться до нуля в отсутствии других. Например, слабые пароли сводят на нет существующие в системе механизмы разграничения доступа, антивирусные средства и средства обнаружения вторжений требуют непрерывного обновления сигнатур, а политики безопасности не работают в отсутствии программы обучения и повышения осведомленности персонала.

Приемлемая величина остаточного риска не должна превышать максимально допустимый уровень риска, утвержденный руководством, который может быть сопоставим, например, со стандартными издержками одного производственного процесса организации. После выбора способов обработки риска следует оценить остаточный риск, и если этот риск не приемлем, тогда необходимо повторить обработку.

В случае если оценочная величина остаточного риска превышает максимально допустимый уровень риска, то для его уменьшения должны быть выбраны дополнительные механизмы контроля, обеспечивающие наилучший возврат инвестиций и позволяющие уменьшить остаточный риск до приемлемого уровня.

В случае невозможности либо экономической нецелесообразности уменьшения риска до приемлемого уровня должны быть рассмотрены варианты передачи данного риска третьей стороне, в качестве которой может выступать страховая компания или компания, предоставляющая услуги по аутсорсингу ИТ процессов и сервисов безопасности, а также варианты избежания риска, связанные с отказом от рискованных операций либо их заменой на менее рискованные.

В случае отсутствия других приемлемых вариантов обработки риска, превышающего установленный в организации максимально допустимый уровень, руководством компании может быть принято решение о принятии данного риска.

Способы обработки риска

После того как риск был оценен, руководством организации должно быть принято решение о способе обработки этого риска.

Помимо предполагаемых потерь в результате инцидентов безопасности, организация должна также рассмотреть затраты на реализацию решения по обработке риска в сравнении с отсутствием каких-либо действий и прогнозируемыми потерями. Организация должна убедиться в том, что она достигает оптимального баланса между достижением определенного уровня безопасности и получением связанных с этим преимуществ, при правильном

инвестировании – с одной стороны, и сохранением рентабельности, успешности, эффективности и конкурентоспособности – с другой.

Существует четыре возможных способа обработки риска:

- принятие (сохранение) риска;
- уменьшение риска;
- передача риска;
- избежание риска.

Принятие риска

На решение о принятии (сохранении) риска оказывают влияние различные обстоятельства. Например, стартующий высокотехнологичный бизнес может принимать более высокие риски, нежели солидная организация традиционного профиля.

Основными факторами, влияющими на решение о принятии рисков,являются:

возможные последствия осуществления риска, т.е. расходы организации в каждом случае, когда это происходит;

ожидаемая частота подобных событий.

Количественные оценки этих факторов, как мы видели, являются очень неточными и субъективными, поэтому лица, принимающие решение, должны осторожно взвешивать точность и достоверность информации, на основании которой они принимают решение, и величину потерь, которую они готовы принять.

К числу субъективных факторов, оказывающих влияние на принятие решений по рискам, относятся в том числе:

готовность к принятию рисков (также известная как терпимость или склонность к риску);

простота реализации механизма контроля;

доступные финансовые, кадровые и информационные ресурсы;

существующие деловые/технологические приоритеты;

политика организации и руководства, например, в отношении следования тем или иным требованиям.

Критерии принятия рисков

Каждая организация должна установить критерии принятия рисков, определяющие максимально допустимый уровень остаточного риска, а также возможные исключения для определенных рисков при определенных обстоятельствах.

Риски, превышающие установленный руководством организации допустимый уровень, – это те риски, которые являются неприемлемыми для бизнеса, а связанная с ними деятельность – слишком рискованной. Все остальные риски, ниже этого уровня, являются допустимыми и могут быть приняты без дальнейшей обработки.

На практике многие риски занимают промежуточное положение между однозначно приемлемыми и очевидно неприемлемыми. Такие риски также нуждаются в обработке, хотя и не в первую очередь, и могут быть снижены при обеспечении хорошего возврата инвестиций. Поэтому в дополнение к максимально допустимому уровню остаточного риска мы также используем уровень однозначно приемлемого риска.

Уровни принятия риска:

- Низкий риск (уровень риска: от 0 до 2) – однозначно приемлемые риски, составляющие обычныйрисковый фон организации.
- Средний риск (уровень риска: от 3 до 5) – потенциально приемлемые риски, уменьшение которых, однако, может дать положительный экономический эффект. Эти риски обычно нуждаются в обработке, но не в первую очередь.
- Высокий риск (уровень риска: от 6 до 8) – неприемлемые риски, нуждающиеся в скорейшей обработке. Сохранение данных рисков руководство организации считает крайне рискованным для своего бизнеса.

В ситуации, когда за разные риски отвечают разные подразделения организации, используемые критерии принятия рисков требуют согласования между этими подразделениями, а также с руководством организации. В противном случае возникает ситуация, при которой организация применяет разные критерии принятия рисков для разных областей контроля, что приводит к недооценке одних видов рисков и переоценке других.

На рисунке 3.3.2 показано, как выглядят несогласованные критерии принятия рисков (1 – информационная безопасность, 2 – охрана труда, 3 – финансовый риск, 4 – операционный риск). В данном случае организация переоценивает риски информационной безопасности и недооценивает прочие операционные риски. Такая ситуация порождает определенные трудности с принятием решения по рискам.

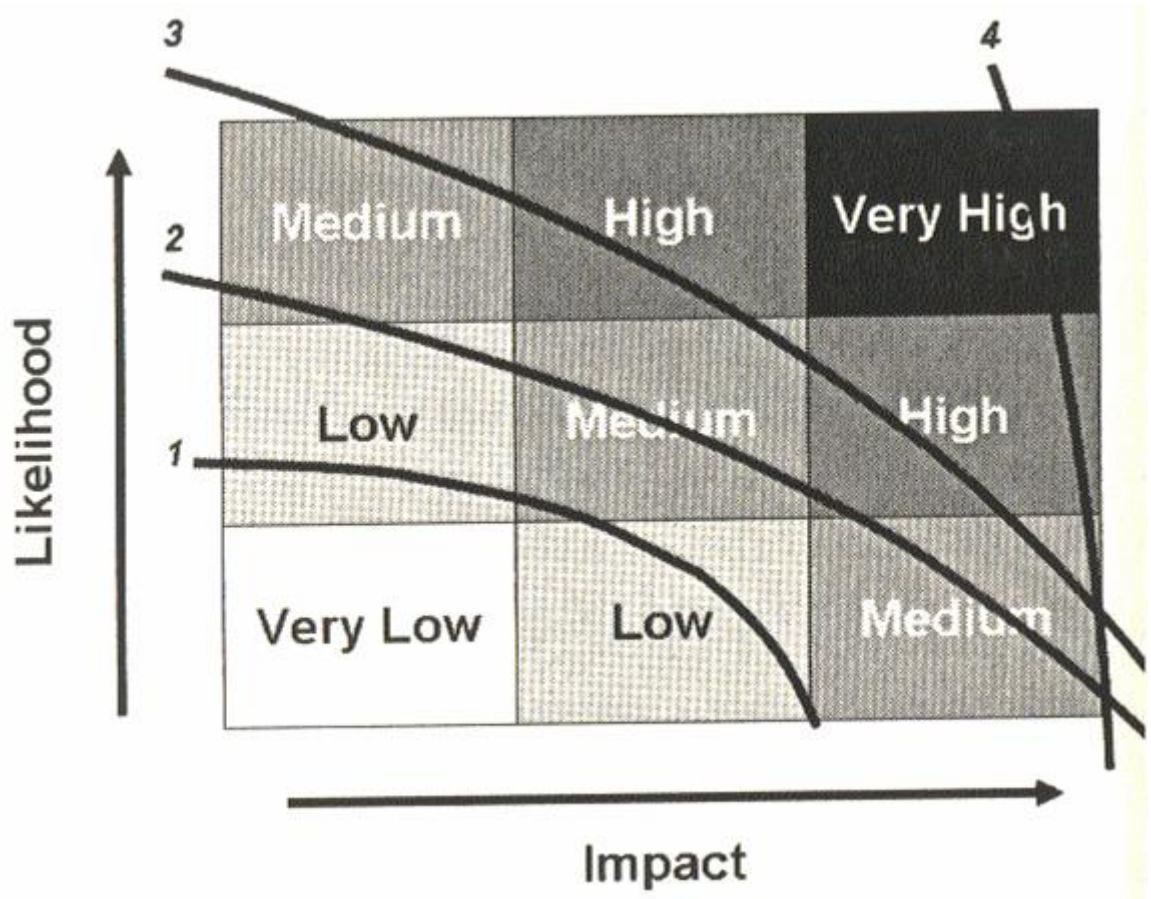

Рис. 3.3.2. Процесс обработки рисков.

Если организация применяет согласованные критерии принятия риска для всех областей деятельности в рамках единой системы управления рисками (ERM-системы), руководству значительно проще принимать решения по рискам. Это позволит избежать опасных последствий недооценки определенных видов рисков и необоснованных затрат на уменьшение рисков, которые, напротив, были переоценены.

Уменьшение риска

Если риск неприемлем, то обычно в первую очередь рассматривается вопрос о его уменьшении до уровня, который был определен как максимально допустимый, путем применения соответствующих механизмов контроля.

Одним из наиболее авторитетных источников для выбора механизмов контроля служат международные стандарты ISO 27001 и ISO 27002, предоставляющие описание и руководство по внедрению для каждого механизма контроля. В стандарте ISO 15408 «Общие критерии оценки безопасности информационных технологий» и разработанных на его основе профилях защиты можно найти соответствующие требования и подобрать спецификацию практически для любых программно-технических механизмов контроля. Заслуживает также внимания немецкий стандарт в области ИТ безопасности BSI/IT Baseline Protection Manual.

Механизмами контроля в международных стандартах называют любые меры, направленные на уменьшение риска. Уменьшать риски можно следующими способами:

- уменьшением вероятности воздействия угрозы на активы;
- ликвидацией имеющихся уязвимостей;
- уменьшением вероятности использования уязвимости;
- уменьшением возможного ущерба в случае осуществления риска путем обнаружения нежелательных событий, реагирования и восстановления после них.

Какой из этих способов (или их комбинацию) организация выбирает для защиты своих активов, зависит от требований бизнеса, внешней среды и обстоятельств. Выбор механизмов контроля должен быть обоснован. Основными критериями такого выбора служат его реализуемость, эффективность в достижении целей контроля и экономическая целесообразность, измеряемая коэффициентом возврата инвестиций (ROI). Каким образом определяется ROI, мы рассмотрим ниже в разделе «Оценка возврата инвестиций в информационную безопасность».

Не существует универсального или достаточно общего подхода к выбору целей и механизмов контроля. Процесс выбора, вероятно, будет включать в себя большое количество этапов принятия решения, консультации и обсуждения с представителями бизнеса и ключевыми лицами, а также анализ целей бизнеса. Процесс выбора должен базироваться на четко определенном наборе целей и задач бизнеса или его миссии и произвести результаты, которые наилучшим образом подходят для организации в терминах требований бизнеса по защите его активов и инвестиций, культуры организации и ее терпимости к риску.

Выбор механизмов контроля опирается на результаты оценки риска. Анализ уязвимости или угрозы может показать, где требуется защита и какие формы она должна принимать. Любые подобные ссылки на оценку рисков должны быть документированы с целью обоснования выбора (либо исключения) механизмов контроля. Документирование выбранных механизмов контроля, наряду с целями контроля, для достижения которых они предназначены, помогает организации далее непрерывно отслеживать ход внедрения и эффективность механизмов контроля.

При выборе механизмов контроля должно учитываться большое количество других факторов, включая:

- простоту внедрения и эксплуатации механизма контроля;
- надежность и воспроизводимость механизма контроля (является ли он документированным, исполняется он вручную или запрограммирован);
- относительную силу механизмов контроля по сравнению с другими мерами;

- типы выполняемых функций (предотвращение, сдерживание, обнаружение, восстановление, исправление, мониторинг или оповещение).
- На выбор механизмов контроля могут повлиять следующие ограничения:
- время реализации– может быть неприемлемым, например, превышать жизненный цикл процесса, для которого требуется уменьшить риск;
- законодательные– ограничения на использование средств шифрования;
- кадровые– доступность специализированного персонала;
- этические– не во всех организациях уместна перлюстрация почты, а сообщения о подозрительных действиях в ряде случаев могут трактоваться как доносительство;
- культурные– досмотр сумок можно ввести в Европе, но это недопустимо в странах Ближнего Востока. Успешность внедрения в значительной степени зависит от поддержки со стороны персонала;
- операционные– необходимость обеспечения непрерывной доступности системы 24 часа в сутки.

Передача риска

Передача риска может быть выбрана в случае, если сложно уменьшить риск до приемлемого уровня либо если передача этого риска третьей стороне экономически более оправдана.

Основными механизмами передачи риска являются страхование и аутсорсинг.Для передачи риска годятся также любые договорные отношения, позволяющие разделять ответственность и перекладывать риск на внешнюю сторону (партнеров, клиентов и т.п.). Не стоит, однако, рассматривать государство в качестве такой внешней стороны. Передать риск государству достаточно проблематично. Предлагая, а чаще всего навязывая, бизнесу систему лицензирования, сертификации и аттестации, государство при этом не принимает на себя соответствующие риски бизнеса. Для аттестованных систем никаких дополнительных гарантий и компенсации ущерба не предоставляется, наличие лицензий и сертификатов не является гарантией безопасности. Не получится разделить ответственность также и с независимыми негосударственными органами по сертификации, т.к. эти органы лишь декларируют соответствие определенным требованиям.

Традиционным механизмом передачи риска является страхование. Страховщики делают бизнес на чужих рисках, принимая на себя эти риски и получая за это страховую премию. Компенсация убытков предоставляется в том случае, если осуществляется риск, который укладывается в рамки страхового покрытия. Успех их бизнеса определяется точностью прогнозирования среднегодового ущерба, которые должен быть существенно меньше страховой премии.

Однако даже при страховании присутствует элемент остаточного риска, поскольку будут существовать условия и исключения, применяемые в зависимости от типа происшествия, для которых компенсация не будет предоставляться. Поэтому необходимо тщательно анализировать передачу риска при помощи страхования для того, чтобы определить, какая часть риска реально передается. Следует также учитывать, что страхование обычно не имеет дело с нефинансовыми последствиями и не предоставляет немедленной компенсации в случае инцидента.

Другой возможностью является использование третьих сторон или партнеров по аутсорсингу для управления неосновными бизнес-процессами организации. В этом случае необходимо позаботиться о получении гарантий того, что все требования безопасности, цели и механизмы контроля включены в соответствующие договора для обеспечения достаточного уровня безопасности.

Кроме того, следует определить требования безопасности вместе с конкретными показателями эффективности в соглашениях об уровне сервиса таким образом, чтобы эффективность предпринимаемых мер безопасности могла быть измерена. Необходимо принимать во внимание, что здесь также присутствует остаточный риск, заключающийся в том, что окончательная ответственность за безопасность аутсорсинговой информации и средств ее обработки остается за вашей организацией, а также, что через аутсорсинг могут привноситься новые риски, которые также должны оцениваться и контролироваться.

Избежание риска

Прежде чем планировать расходы на уменьшение или передачу риска, возможно, стоит задуматься, нельзя ли избежать риска путем реорганизации бизнес-процесса, например путем выбора иных способов передачи, хранения или обработки информации.

Избежание рискаозначает любые действия, при которых изменяются способы ведения бизнеса для того, чтобы избежать осуществления риска. Например, избежание риска может быть достигнуто путем:

отказа от определенных бизнес-активностей (например, неиспользования возможностей, предоставляемых электронной коммерцией, или неиспользования Интернет для осуществления некоторых операций);

перемещения ресурсов из зоны риска (например, отказ от хранения конфиденциальных файлов в Интранет-сети организации или перемещение ресурсов из зон, недостаточно защищенных физически);

принятия решения о том, чтобы не обрабатывать конкретную конфиденциальную информацию, например, совместно с третьей стороной в случае, если адекватный уровень защиты не может быть гарантирован.

Избежание риска должно быть сбалансировано с потребностями бизнеса и финансовыми целями. Например, использование Интернет или электронной коммерции может являться неизбежным для организации в связи с деловой необходимостью, несмотря на озабоченность по поводу хакеров, или с точки

зрения бизнеса может быть неосуществимо перемещение определенных ресурсов в более надежное место. В таких ситуациях должны рассматриваться другие варианты, такие как передача или уменьшение риска.

Принятие решения по обработке рисков – ключевой и наиболее ответственный момент в процессе управления рисками. Решение по рискам – это бизнес-решение, как правило, оказывающее влияние на всю дальнейшую деятельность организации. Поэтому приниматься это решение должно лицом, находящимся на соответствующем уровне властной иерархии и отвечающим за весь бизнес или ту его часть, которая подвергается риску. Руководитель информационной безопасности должен принимать решения на своем уровне относительно того, как оптимальным образом воплотить в жизнь решения своего руководства по обработке информационных рисков.

Для того чтобы руководство могло принять правильное решение, сотрудник, отвечающий за управление рисками в организации, должен предоставить ему соответствующую информацию. Решение по бизнес-рискам должен принимать руководитель бизнеса либо лицо, которому он делегирует ответственность за определенные направления бизнеса. Руководитель службы информационной безопасности или риск-менеджер готовит решение по рискам для руководства организации.

Форма представления руководству организации информации для принятия решения по рискам определяется стандартным алгоритмом делового общения и может включать в себя следующие основные пункты:

Сообщение о проблеме:в чем заключается угроза для бизнеса (источник, объект, способ реализации) и в чем причина ее существования?

Степень серьезности проблемы:чем это грозит организации, ее сотрудникам, руководству, акционерам?

Предлагаемое решение:что предлагается сделать для исправления ситуации, во сколько это обойдется, кто это должен делать и что требуется непосредственно от руководства? (Используя оценки ROI для обоснования предлагаемого решения).

Альтернативные решения:какие еще способы решения проблемы существуют (альтернативы есть всегда, и у руководства должна быть возможность выбора). Для сравнения альтернативных решений, помимо экономического обоснования (оценок ROI), могут также использоваться соображения о времени реализации решения, учитываться морально-этические аспекты и любые другие факторы, которые целесообразно принимать во внимание.

Каков остаточный риск?Не превышает ли он приемлемого уровня? Если уровень остаточного риска не устраивает руководство, то потребуется дополнительная обработка риска.

Такой обстоятельный доклад о рисках, подкрепленный реестром информационных рисков и планом обработки рисков, обоснованным с точки зрения возврата инвестиций, и опирающийся на согласованные с руководством

критерии оценки ущерба и принятия рисков, позволяет принимать наиболее взвешенные и эффективные решения по рискам. В этом случае СУИР предоставляет руководству организации эффективный механизм подготовки и принятия решений, превращая эту задачу из крайне запутанной проблемы, требующей для своего разрешения сильной интуиции и умения принимать нестандартные решения в условиях недостатка и противоречивости исходных данных, в обычную повседневную рутину. Функция руководства по существу сводится лишь к контролю предлагаемых решений, корректировкам бюджета, согласованию сроков и выделяемых ресурсов. В некоторых случаях от руководства потребуется политическая воля для принятия остаточных рисков, не укладывающихся в установленные рамки, либо изменения критериев принятия рисков.

Принятие взвешенных и эффективных решений в условиях нечеткой и неполной информации – основная функция любого руководителя. Процесс этот достаточно субъективный. Такой же субъективный характер носят и решения, принимаемые руководителями. Информационная безопасность здесь исключением не является.

План обработки рисков

После того как решения по обработке рисков были приняты, должны быть определены и спланированы действия по реализации этих решений. Каждое мероприятие должно быть четко определено и разбито на такое количество действий, которое необходимо для четкого распределения ответственности между исполнителями, оценки требований к выделению ресурсов, установки вех и контрольных точек, определения критериев достижения целей и мониторинга продвижения.

Решения руководства по обработке рисков оформляются в виде «Плана обработки рисков». Этот документ является производным от «Реестра информационных рисков», определяющим для каждой группы угроз и уязвимостей перечень мер по обработке риска, позволяющих уменьшить максимальный для данной группы угроз уровень риска до уровня остаточного риска, приемлемого для организации. План обработки рисков также определяет сроки реализации, выделяемые ресурсы и ответственных исполнителей.

Таблица 3.3.1 Пример плана обработки рисков

№	Угрозы	Уязвимости	Максимальный уровень риска	Меры по обработке риска	Остаточный уровень риска	Дата	Комментарии, ресурсы, ответственные
Обработка рисков офисной сети							
Физические риски							
1	Кража компьютерного оборудования и носителей информации инсайдерами Физический НСД в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.	Не производится регистрация оборудования и информационных носителей, выносимых за пределы территории организации. Отсутствуют правила работы в зонах безопасности. При приеме на работу не производится проверка истории кандидатов.	5	Разработать систему мер, ограничивающих неконтролируемое использование внешних носителей и мобильных устройств вне офиса. Реализовать меры по проверке кредитной истории кандидатов для критичных должностей. Разработать правила работы в зонах безопасности.	4		
2	Кража компьютерного оборудования и носителей	Контроль посетителей на ресепшине не производится.	5	Разработать политику обеспечения физической безопасности, предусматривающую, в том числе,	4		

Процесс планирования должен включать в себя идентификацию ключевых владельцев активов и бизнес-процессов, консультирование с ними по выделению временных, финансовых и прочих ресурсов на реализацию плана обработки рисков, а также получение санкции руководства соответствующего уровня на использование ресурсов.

Разработка и реализация плана обработки рисков включает в себя следующие меры:

- определение последовательности мероприятий по реализации принятых решений по обработке рисков;
- детализацию и приоритетизацию мероприятий по обработке рисков;
- распределение ответственности между исполнителями;
- выделение необходимых ресурсов;
- определение вех и контрольных точек;
- определение критериев достижения целей;
- мониторинг продвижения.

Должны быть правильно расставлены приоритеты по реализации мер обработки риска. Время, когда может предприниматься каждое действие, зависит от его абсолютного приоритета по отношению к другим действиям, доступности ресурсов (включая финансовые и кадровые ресурсы), а также от мероприятий, которые должны быть завершены, прежде чем процесс может быть запущен. План обработки рисков должен быть скоординирован с другими бизнес-планами. Любые зависимости между этими планами должны быть идентифицированы.

Приоритетизация мер по обработке рисков может осуществляться следующим образом:

1. Все контрмеры разделяются на группы по уровню риска, для уменьшения которого они предназначены. Наивысший приоритет присваивается контрмерам, служащим для уменьшения самых больших рисков.
2. В каждой группе на первое место ставятся те меры, которые быстрее и проще реализовать и которые дают скорейший эффект.
3. Повышается приоритет контрмер, обеспечивающих наибольший возврат инвестиций ROI.
4. Первичным контрмерам, от которых зависит успешность реализации других контрмер, присваивается более высокий приоритет.
5. Учитываются все прочие соображения, способные повлиять на порядок реализации контрмер, включая связь с другими планами, доступность тех или иных ресурсов, политические, экономические и прочие соображения.

На выходе данного процесса получаем приоритетный перечень мер по обработке рисков, на базе которого производится дальнейшее более детальное планирование, выделение ресурсов и реализация решений по управлению рисками.

Координация всех шагов по реализации плана обработки рисков (включая приобретение, внедрение, тестирование механизмов безопасности, заключение договоров страхования и аутсорсинга и т.п.) осуществляется менеджером информационной безопасности или риск-менеджером, который должен контролировать, чтобы реализация мероприятий осуществлялась в соответствии с планом, с надлежащим качеством и в рамках выделенных финансовых, временных и кадровых ресурсов. При внедрении контрмер в информационную систему должно проводиться тестирование с целью подтверждения надежности и работоспособности реализованных механизмов безопасности, а также измерение эффективности их функционирования.

3.4. Политика информационной безопасности

Политика информационной безопасности (ПИБ) - совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые направлены на защиту ценной информации.

Назначение политика информационной безопасности :

-- формулирование целей и задач информационной безопасности организации с точки зрения бизнеса (позволяет определить это для руководства и продемонстрировать поддержку руководством значимости ИБ),

-- определение правил организации работы в компании для минимизации рисков информационной безопасности и повышения эффективности бизнеса.

Требования к политике информационной безопасности:

-- Политика должна быть утверждена высшим административным органом компании (генеральный директор, совет директоров и т.п.) для демонстрации поддержки руководства.

-- Политика ИБ должна быть написана понятным языком для конечных пользователей и руководства компании и быть по возможности краткой.

-- Политика ИБ должна определять цели ИБ, способы их достижения и ответственность. Технические подробности реализации способов содержатся в инструкциях и регламентах, на которые даются ссылки в Политике.

-- Минимизация влияния политики безопасности на производственный процесс.

-- Непрерывность обучения сотрудников и руководства организации в вопросах обеспечения ИБ

-- Непрерывный контроль выполнения правил политики безопасности на этапе внедрения и в дальнейшем.

-- Постоянное совершенствование политик безопасности.

-- Согласованность во взглядах и создание корпоративной культуры безопасности.

Предлагается следующая структура ПИБ:

· Общие положения (ссылки на законы, нормативные акты и др.руководящие документы, которым подчиняется деятельность организации),

· Подтверждение значимости ИБ для организации и формулирование целей защиты информации с точки зрения бизнеса организации (выполнение требований законодательства и др. норм, удовлетворение ожиданий клиентов и партнеров, повышение конкурентоспособности, финансовой стабильности, имиджа организации).

· Описание стратегии организации по обеспечению информационной безопасности (например, выполнение требований законодательства, оценка и управление рисками).

· Область применения ПИБ (например, ПИБ обязательна для выполнения всеми сотрудниками и руководством организации, или отдельного филиала, или сотрудниками, использующими ноутбуки)

· Описание объекта защиты (защищаемые ресурсы - информация различных категорий, информационная инфраструктура и т.д.)

· Цели и задачи обеспечения информационной безопасности (например, снижение угроз ИБ до приемлемого уровня, выявление потенциальных угроз и уязвимостей ИБ, предотвращение инцидентов ИБ)

· Краткое разъяснение принципов политики ИБ:

- подход к построению системы управления ИБ,
- требования к подготовке и осведомленности персонала в области ИБ,
- последствия и ответственность за нарушение ПИБ,
- подход к управлению рисками,
- определение оргструктуры, общих и специальных обязанностей по управлению ИБ, включая отчеты об инцидентах,
- ссылки на документацию, которая может поддержать политику, например, частные политики и процедуры в области защиты для конкретных

информационных систем или правила защиты, которым должны следовать пользователи.

- механизмы контроля за выполнением положений ПИБ,
- порядок пересмотра и принятия изменений в политике.

После утверждения политики ИБ необходимо:

· Довести положения политики ИБ, подполитик, процедур и инструкций под роспись до сведения рядовых сотрудников при их первоначальном и последующем периодическом обучении и информировании;

· Разработать процедуры, инструкции и т.д., уточняющие и дополняющие политику

· Периодически анализировать политику для поддержки ее адекватности и результативности;

· Проводить периодический аудит на выполнение сотрудниками положений политики с предоставлением отчета Руководству организации.

· Кроме того, в должностные инструкции ответственного персонала, положения о подразделениях, контрактные обязательства организации должны быть включены обязанности по обеспечению информационной безопасности.

3.5. Осведомленность сотрудников по информационной безопасности

Осведомленность сотрудников в теме ИБ является одним из самых важных аспектов Информационной безопасности любой компании. Применение различных технических средств защиты и контроля не способно в полной мере защитить компанию от человеческой ошибки. Порой сотрудники компании не всегда представляют себе опасность и возможные риски цифрового мира. В тоже время, доступность и распространение хакерских инструментов, развитие техник социальной инженерии, простое незнание сотрудника о современных угрозах лишь увеличивают возможность атаки на компанию и возможный ущерб.

Именно поэтому разработка и внедрение мероприятий по увеличению осведомленности сотрудников является важным шагов со стороны представителей ИБ/ИТ.

Рассмотрим некоторые возможные мероприятия, направленные на повышение знаний сотрудников компании в этой многогранной области.

Тренинги для новых сотрудников

Текучка кадров есть в каждой компании и чем больше компания, тем она выше. Новые сотрудники не знают всех правил и внутренних процедур, что создает для компании дополнительные риски. В качестве меры снижения этих

рисков можно рассмотреть возможность проведения тренинга для новых сотрудников.

Проведение таких тренингов позволяет представителям различных департаментов рассказать об их работе, внутренних процедурах и особенностях взаимодействиях. К примеру, отдел кадров может рассказать о том, как сотрудник может заказать справки, PR-отдел - кто и как взаимодействует с прессой, ИТ-отдел - правила обращения сотрудников и заказа услуг и т.д..

На таком тренинге сотрудники ИБ могут рассказать сотрудникам об общих правилах безопасности, об особенностях взаимодействия сотрудников с представителями службы ИБ, о том, что делать в случае получения подозрительного письма или вируса. Выступление, поддерживаемое примерами из реальной жизни и практики ИБшников, позволит вновь прибывшим "бойцам" лучше понять причины установленных правил и ограничений, а также, что нужно предпринять в случае заражения вирусом или получения фишингового письма.

Такая лекция не должна быть тяжелой и долгой, по этому лучше ограничиться 20-30 минутами.

В крупных компаниях сотрудники могут иметь "уникальные" вопросы, связанные с прямыми обязанностями или проектами, над которыми они работают. Именно по этому, небольшая сессия вопросов и ответов после лекции позволит сотрудникам получить нужную информацию, ну или хотя бы имена людей/отделов, которые могут помочь.

Ежегодные тренинги

Отличной практикой для предотвращения ИБ инцидентов является ежегодный тренинг. Здесь у сотрудников ИБ значительно больше свободы, т.к. формат и содержимое таких тренингов не ограничивается исключительно внутренними правилами. В ходе такого тренинга могут быть затронуты более глобальные темы, такие как социальная инженерия, фишинг, правила безопасности во время путешествий, безопасное использование интернета и т.д.

При проведении таких тренингов в формате лекций могут возникнуть определенные организационные трудности, к примеру, сложно собрать большое количество людей в одном месте, даже проведение нескольких сессий не всегда способно охватить всех сотрудников. Пожалуй, лучшим решением в этой ситуации будет создание курса на базе e-learning системы с проверочным тестом. Плюсы такого подхода очевидны:

• Курс может быть интереснее, за счет использования видео материалов, интерактивных элементов и др.

• Сотрудник сам выбирает время для прохождения курса;

• Получение статистики для дальнейшего анализы.

Но, к сожалению, данный подход требует определенных затрат, как временных, так и финансовых.

Подготовка такого рода тренинга начинается задолго до его публикации и зависит от предоставляемых самой компанией возможностей и бюджета. Если компания обладает достаточными финансовыми ресурсами, такой проект может быть отдан на аутсорсинг под контролем представителей ИБ. В этом случае, качество контента (как и конечный продукт) может быть выше. А в случае международной компании, контент (закадровый голос и текст) могут быть представлены на нескольких языках.

Если же компания не имеет возможности оплатить услуги сторонней организации, всегда можно найти вариант проще. К примеру, подготовленные презентации или видео на основе этих презентаций, размещенные на внутренних ресурсах позволят сотрудникам просмотреть подготовленный материал и выполнить тест. К сожалению, сбор статистики и контроль в этом случае весьма затруднителен. Безусловно, можно поместить проверочный тест в системах, куда имеют доступ все сотрудники компании - портал заказа ИТ-услуг или портал взаимодействия с HR , но это во многом зависит от используемых систем и от инфраструктуры компании.

Демонстрации атак

Одной из самых сложных в реализации, но в то же время, самой зрелищной для публики является демонстрация "хакерских" атак. Видео с такими демонстрациями свободно распространяются в интернете, так что найти их не составит труда, а практически весь необходимый набор программ включает в себя Kali Linux и ему подобные дистрибутивы.

Не стоит демонстрировать какие то сложные или долгие для реализации атаки, рекомендуется начинать с чего- то простого, к примеру, перехват нешифрованного трафика в одной сети или автоматическое подключение к публичным сетям и возможные проблемы, связанные с этим. Цель – не показать какой вы мастер, а показать, насколько опасен, может быть неосмотрительный подход к передаче данных и к интернету в целом. Идеально – это научить сотрудника думать и заботиться о своей безопасности и безопасности данных компании.

Хороший сценарий поможет организовать и продумать переходы от вступительной речи к демонстрации. Вступительная часть, в ходе которой может быть описание реальной ситуации, в которой может оказать каждый, является очень важным элементом для самих сотрудников. Важно помнить, что большая часть аудитории - это люди, не слишком хорошо разбирающихся в технических нюансах.

Во вступительной части лучше рассказать о каком-то событии или действии знакомом каждому: нет человек, который бы не подключался к бесплатной WiFi сети в аэропорту или на вокзале. Но знает ли он возможные последствия использования данных сетей? Скорее нет, чем да. Именно это и можно продемонстрировать аудитории во второй части: перехват трафика, кража данных, фишинговые сайты и прочее. В заключительной части крайне желательно рассказать сотрудникам о том, как защитить себя от этих угроз. Само собой после демонстрации у коллег возникнут вопросы и, чем сложнее была демонстрация, тем больше будет вопросов и к этому надо быть готовым.

4. Технологии защиты

4.1. Аутентификация. Управление доступом.

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

(Заметим в скобках, что происхождение русскоязычного термина "аутентификация" не совсем понятно. Английское "authentication" скорее можно прочитать как "аутентикация"; трудно сказать, откуда в середине взялось еще "фи" - может, из идентификации? Тем не менее, термин устоялся, он закреплен в Руководящих документах Гостехкомиссии России, использован в многочисленных публикациях, поэтому исправить его уже невозможно.)

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации - процедура входа пользователя в систему.

В сетевой среде, когда стороны аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

что служит аутентификатором (то есть используется для подтверждения подлинности субъекта);

как организован (и защищен) обмен данными аутентификации.

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);

нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);

нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

В открытой сетевой среде между сторонами /аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения и/или воспроизведения данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

Надежная идентификация и затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократнаяаутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств аутентификации.

Любопытно отметить, что сервис аутентификации может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

Парольная аутентификация

Главное достоинство парольной аутентификации - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по

совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Известна классическая история про советского разведчика Рихарда Зорге, объект внимания которого через слово говорил "карамба"; разумеется, этим же словом открывался сверхсекретный сейф.

Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Ввод пароля можно подсмотреть. Иногда для подглядывания используются даже оптические приборы.

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

Пароль можно угадать "методом грубой силы", используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен).

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);

управление сроком действия паролей, их периодическая смена;

ограничение доступа к файлу паролей;

ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");

обучение пользователей;

использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

Одноразовые пароли

Рассмотренные выше пароли можно назвать многоразовыми; их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются одноразовые пароли.

Наиболее известным программным генератором одноразовых паролей является система SecurID компании RSA. Идея этой системы состоит в следующем. Пусть имеется односторонняя функция f (то есть функция,

вычислить обратную которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и серверу аутентификации. Пусть, далее, имеется секретный ключ K, известный только пользователю.

На этапе начального администрирования пользователя функция f применяется к ключу K n раз, после чего результат сохраняется на сервере. После этого процедура проверки подлинности пользователя выглядит следующим образом:

сервер присылает на пользовательскую систему число (n-1);

пользователь применяет функцию f к секретному ключу K (n-1) раз и отправляет результат по сети на сервер аутентификации;

сервер применяет функцию f к полученному от пользователя значению и сравнивает результат с ранее сохраненной величиной. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик (n).

На самом деле реализация устроена чуть сложнее (кроме счетчика, сервер посылает затравочное значение, используемое функцией f), но для нас сейчас это не важно. Поскольку функция f необратима, перехват пароля, равно как и получение доступа к серверу аутентификации, не позволяют узнать секретный ключ K и предсказать следующий одноразовый пароль.

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или специальные интеллектуальные карты (с практической точки зрения такие пароли можно считать одноразовыми). Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронизированы.

Сервер аутентификации Kerberos

Kerberos - это программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

Kerberos предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены субъекты - пользователи, а также клиентские и серверные программные системы. Каждый субъект обладает секретным ключом. Чтобы субъект C мог доказать свою подлинность субъекту S (без этого S не станет обслуживать C), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. C не может просто послать S свой секретный ключ, во-первых, потому, что сеть открыта (доступна для пассивного и активного прослушивания), а, во-вторых, потому, что S не знает (и не должен знать) секретный ключ C. Требуется менее прямолинейный способ демонстрации знания секретного ключа.

Система Kerberos представляет собой доверенную третью сторону (то есть сторону, которой доверяют все), владеющую секретными ключами

обслуживаемых субъектов и помогающую им в попарной проверке подлинности.

Чтобы с помощью Kerberos получить доступ к S (обычно это сервер), C (как правило - клиент) посылает Kerberos запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ Kerberos возвращает так называемый билет, зашифрованный секретным ключом сервера, и копию части информации из билета, зашифрованную секретным ключом клиента. Клиент должен расшифровать вторую порцию данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом. Совпадение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные (ведь содержимое билета никому, кроме сервера и Kerberos, недоступно), то есть продемонстрировал знание секретного ключа. Значит, клиент - именно тот, за кого себя выдает. Подчеркнем, что секретные ключи в процессе проверки подлинности не передавались по сети (даже в зашифрованном виде) - они только использовались для шифрования. Как организован первоначальный обмен ключами между Kerberos и субъектами и как субъекты хранят свои секретные ключи - вопрос отдельный.

Проиллюстрируем описанную процедуру на рис 4.1.1.

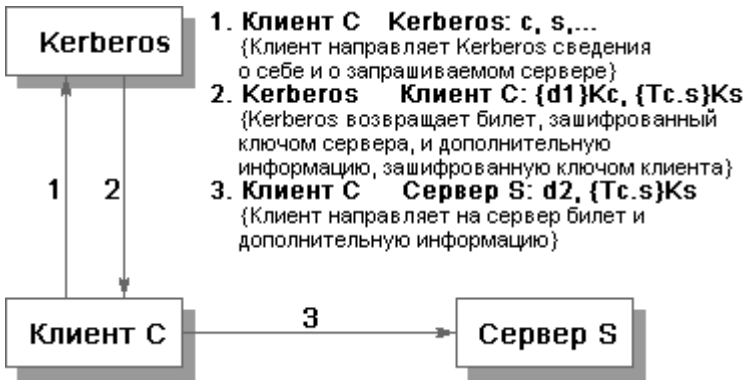

Рис. 4.1.1 Проверка сервером S подлинности клиента C.

Здесь c и s - сведения (например, имя), соответственно, о клиенте и сервере, d1 и d2 - дополнительная (по отношению к билету) информация, Tc.s - билет для клиента C на обслуживание у сервера S, Kc и Ks - секретные ключи клиента и сервера, {info}K - информация info, зашифрованная ключом K.

Kerberos не только устойчив к сетевым угрозам, но и поддерживает концепцию единого входа в сеть.

Аутентификация с помощью биометрических данных

Биометрия представляет собой совокупность автоматизированных методов аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

Биометрией во всем мире занимаются очень давно, однако долгое время все, что было связано с ней, отличалось сложностью и дороговизной. В последнее время спрос на биометрические продукты, в первую очередь в связи с развитием электронной коммерции, постоянно и весьма интенсивно растет. Это понятно, поскольку с точки зрения пользователя гораздо удобнее предъявить себя самого, чем что-то запоминать. Спрос рождает предложение, и на рынке появились относительно недорогие аппаратно-программные продукты, ориентированные в основном на распознавание отпечатков пальцев.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для аутентификации пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

Обычно биометрию применяют вместе с другими аутентификаторами, такими, например, как интеллектуальные карты. Иногда биометрическая аутентификация является лишь первым рубежом защиты и служит для активизации интеллектуальных карт, хранящих криптографические секреты; в таком случае биометрический шаблон хранится на той же карте.

На наш взгляд, к биометрии следует относиться весьма осторожно. Необходимо учитывать, что она подвержена тем же угрозам, что и другие методы аутентификации. Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти. Во-вторых, биометрические методы не более надежны, чем база данных шаблонов. В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в "полевых" условиях, когда, например к устройству сканирования роговицы могут поднести муляж и т.п. В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

Но главная опасность состоит в том, что любая "пробоина" для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей системы.

Авторизация или Управление доступом

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). В данном разделе речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах - объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа. Фрагмент матрицы может выглядеть, например, так:

Таблица 4.1.1 Фрагмент матрицы доступа

	Файл	Программа	Линия связи	Реляционная таблица
Пользователь 1	orw с системной консоли	e	rw с 8:00 до 18:00	
Пользователь 2				a

"o" - обозначает разрешение на передачу прав доступа другим пользователям,

"r" - чтение,

"w" - запись,

"e" - выполнение,

"a" - добавление информации

Тема логического управления доступом - одна из сложнейших в области информационной безопасности. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать

и уничтожать. Современные операционные системы могут поддерживать и другие объекты.

Для систем управления реляционными базами данных объект - это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа.

Разнообразие объектов и применимых к ним операций приводит к принципиальной децентрализации логического управления доступом. Каждый сервис должен сам решать, позволить ли конкретному субъекту ту или иную операцию. Теоретически это согласуется с современным объектно-ориентированным подходом, на практике же приводит к значительным трудностям. Главная проблема в том, что ко многим объектам можно получить доступ с помощью разных сервисов (возможно, при этом придется преодолеть некоторые технические трудности). Так, до реляционных таблиц можно добраться не только средствами СУБД, но и путем непосредственного чтения файлов или дисковых разделов, поддерживаемых операционной системой (разобравшись предварительно в структуре хранения объектов базы данных). В результате при задании матрицы доступа нужно принимать во внимание не только принцип распределения привилегий для каждого сервиса, но и существующие связи между сервисами (приходится заботиться о согласованности разных частей матрицы). Аналогичная трудность возникает при экспорте/импорте данных, когда информация о правах доступа, как правило, теряется (поскольку на новом сервисе она не имеет смысла). Следовательно, обмен данными между различными сервисами представляет особую опасность с точки зрения управления доступом, а при проектировании и реализации разнородной конфигурации необходимо позаботиться о согласованном распределении прав доступа субъектов к объектам и о минимизации числа способов экспорта/импорта данных.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой произвольного (или дискреционного) управления доступом;

атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности - основа принудительного (мандатного) управления доступом.

Матрицу доступа, ввиду ее разреженности (большинство клеток - пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Элементами списков могут быть имена групп и шаблоны субъектов, что служит большим подспорьем администратору. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится нечасто.

Списки доступа - исключительно гибкое средство. С их помощью легко выполнить требование о гранулярности прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.

Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления - гибкость. Вообще говоря, для каждой пары "субъект-объект" можно независимо задавать права доступа (особенно легко это делать, если используются списки управления доступом). К сожалению, у "произвольного" подхода есть ряд недостатков. Рассредоточенность управления доступом ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной информацией, эту информацию могут узнать и все остальные пользователи. Следовательно, произвольность управления должна быть дополнена жестким контролем за реализацией избранной политики безопасности.

Второй недостаток, который представляется основным, состоит в том, что права доступа существуют отдельно от данных. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту ее "троянским" аналогом. Подобная "разделенность" прав и данных существенно осложняет проведение несколькими системами согласованной политики безопасности и, главное, делает практически невозможным эффективный контроль согласованности.

Возвращаясь к вопросу представления матрицы доступа, укажем, что для этого можно использовать также функциональный способ, когда матрицу не хранят в явном виде, а каждый раз вычисляют содержимое соответствующих клеток. Например, при принудительном управлении доступом применяется сравнение меток безопасности субъекта и объекта.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек, таких как restricted shell в ОС Unix.

В заключение подчеркнем важность управления доступом не только на уровне операционной системы, но и в рамках других сервисов, входящих в состав современных приложений, а также, насколько это возможно, на "стыках" между сервисами. Здесь на первый план выходит существование единой политики безопасности организации, а также квалифицированное и согласованное системное администрирование.

Ролевое управление доступом

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить.

Таким решением является ролевое управление доступом (РУД). Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности - роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (см. рис. 4.1. 2).

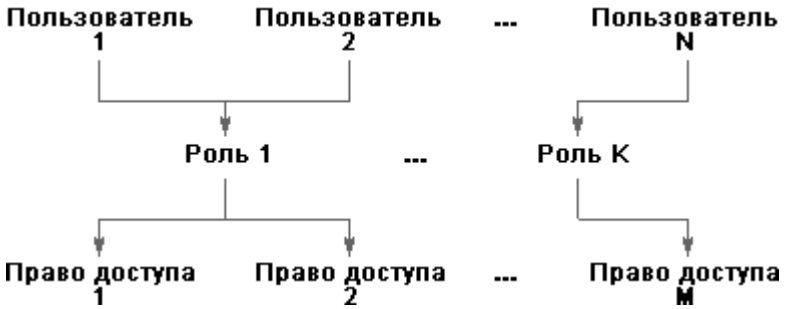

Рис. 4.1.2 Пользователи, объекты и роли.

Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно.

Ролевой доступ развивается много лет (сама идея ролей, разумеется, значительно старше) как на уровне операционных систем, так и в рамках СУБД и других информационных сервисов. В частности, существуют реализации ролевого доступа для Web-серверов.

Ролевое управление доступом оперирует следующими основными понятиями:

пользователь (человек, интеллектуальный автономный агент и т.п.);

сеанс работы пользователя;

роль (обычно определяется в соответствии с организационной структурой);

объект (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);

операция (зависит от объекта; для файлов ОС - чтение, запись, выполнение и т.п.; для таблиц СУБД - вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными);

право доступа (разрешение выполнять определенные операции над определенными объектами).

Ролям приписываются пользователи и права доступа; можно считать, что они (роли) именуют отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многим пользователям; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов.

Между ролями может быть определено отношение частичного порядка, называемое наследованием. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1. Очевидно, что наследование ролей соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям - объекты (экземпляры) классов.

Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить себе формирование иерархии ролей, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), вплоть до роли "руководитель" (что, впрочем, не значит, что руководителю предоставляются неограниченные права; как и другим ролям, в соответствии с принципом минимизации привилегий, этой роли целесообразно разрешить только то, что необходимо для выполнения служебных обязанностей). Фрагмент подобной иерархии ролей показан на рис. 4.1.3.

Рис. 4.1.3. Фрагмент иерархии ролей.

Для реализации еще одного упоминавшегося ранее важного принципа информационной безопасности вводится понятие разделения обязанностей, причем в двух видах: статическом и динамическом.

Статическое разделение обязанностей налагает ограничения на приписывание пользователей ролям. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей. В общем случае данное ограничение задается как пара "множество ролей - число" (где множество состоит, по крайней мере, из двух ролей, а число должно быть больше 1), так что никакой пользователь не может быть приписан указанному (или большему) числу ролей из заданного множества. Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях (здесь число=3).

При наличии наследования ролей ограничение приобретает несколько более сложный вид, но суть остается простой: при проверке членства в ролях нужно учитывать приписывание пользователей ролям-наследницам.

Динамическое разделение обязанностей отличается от статического только тем, что рассматриваются роли, одновременно активные (быть может, в разных сеансах) для данного пользователя (а не те, которым пользователь статически приписан). Например, один пользователь может играть роль и кассира, и контролера, но не одновременно; чтобы стать контролером, он должен сначала закрыть кассу. Тем самым реализуется так называемое временное ограничение доверия, являющееся аспектом минимизации привилегий.

4.2. Безопасность клиетских устройств.Антивирусы.

Для защиты от компьютерных вирусов могут использоваться:

• общие методы и средства защиты информации;

• специализированные программы для защиты от вирусов;

• профилактические меры, позволяющие уменьшить вероятность заражения вирусами.

Общие средства защиты информации полезны не только для защиты от вирусов. Они используются также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя. Существуют две основные разновидности этих средств:

• средства копирования информации (применяются для создания копий файлов и системных областей дисков);

• средства разграничения доступа (предотвращают несанкционированное использование информации, в частности обеспечивают защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей).

При заражении компьютера вирусом важно его обнаружить. К внешним признакам проявления деятельности вирусов можно отнести следующие:

• вывод на экран непредусмотренных сообщений или изображений;

• подача непредусмотренных звуковых сигналов;

• изменение даты и времени модификации файлов;

• исчезновение файлов и каталогов или искажение их содержимого;
• частые зависания и сбои в работе компьютера;
• медленная работа компьютера;
• невозможность загрузки ОС;
• существенное уменьшение размера свободной оперативной памяти;
• прекращение работы или неправильная работа ранее успешно функционировавших программ;
• изменение размеров файлов;
• неожиданное значительное увеличение количества файлов на диске.

Однако следует заметить, что перечисленные выше явления необязательно вызываются действиями вируса, они могут быть следствием и других причин. Поэтому правильная диагностика состояния компьютера всегда затруднена и обычно требует привлечения специализированных программ.

Антивирусные программы

Для обнаружения и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать компьютерные вирусы. Такие программы называются антивирусными. Практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов. Антивирусные программы используют различные методы обнаружения вирусов.

Методы обнаружения вирусов

К основным методам обнаружения компьютерных вирусов можно отнести следующие:

• метод сравнения с эталоном;
• эвристический анализ;
• антивирусный мониторинг;
• метод обнаружения изменений;
• встраивание антивирусов в ВЮ8 компьютера и др.

Метод сравнения с эталоном. Самый простой метод обнаружения заключается в том, что для поиска известных вирусов используются так называемые маски. Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Антивирусная программа последовательно просматривает (сканирует) проверяемые файлы в поиске масок известных вирусов. Антивирусные сканеры способны найти только уже известные вирусы, для которых определена маска.

Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Применение простых сканеров не защищает компьютер от проникновения новых вирусов. Для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить маску, поэтому антивирусные сканеры их не обнаруживают.

Эвристический анализ. Для того чтобы размножаться, компьютерный вирус должен совершать какие-то конкретные действия: копирование в память,

запись в секторы и т. д. Эвристический анализатор (который является частью антивирусного ядра) содержит список таких действий и проверяет программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов. Эвристический анализатор может обнаружить, например, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные в исполнимый файл программы. Обнаружив зараженный файл, анализатор обычно выводит сообщение на экране монитора и делает запись в собственном или системном журнале. В зависимости от настроек, антивирус может также направлять сообщение об обнаруженном вирусе администратору сети. Эвристический анализ позволяет обнаруживать неизвестные ранее вирусы. Первый эвристический анализатор появился в начале 1990-х гг. Практически все современные антивирусные программы реализуют собственные методы эвристического анализа. В качестве примера такой программы можно указать сканер McAffee VirusScan.

Антивирусный мониторинг. Суть данного метода состоит в том, что в памяти компьютера постоянно находится антивирусная программа, осуществляющая мониторинг всех подозрительных действий, выполняемых другими программами. Антивирусный мониторинг позволяет проверять все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты либо компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие. Пример такой программы — сторож Spider Guard, который входит в комплект сканера Doctor Web и выполняет функции антивирусного монитора.

Метод обнаружения изменений. При реализации этого метода антивирусные программы, называемые ревизорами диска, запоминают предварительно характеристики всех областей диска, которые могут подвергнуться нападению, а затем периодически проверяют их. Заражая компьютер, вирус изменяет содержимое жесткого диска: например, дописывает свой код в файл программы или документа, добавляет вызов программы-вируса в файл AUTOEXEC.BAT, изменяет загрузочный сектор, создает файл-спутник. При сопоставлении значений характеристик областей диска антивирусная программа может обнаружить изменения, сделанные как известным, так и неизвестным вирусом.

Встраивание антивирусов в BIOS компьютера. В системные платы компьютеров встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если какая-либо программа пытается изменить содержимое загрузочных секторов, срабатывает защита, и пользователь получает соответствующее предупреждение. Однако эта защита не очень надежна. Известны вирусы, которые пытаются отключить антивирусный контроль BIOS, изменяя некоторые ячейки в энергонезависимой памяти (CMOS-памяти) компьютера.

Виды антивирусных программ

Различают следующие виды антивирусных программ :

• программы-фаги (сканеры);

• программы-ревизоры (CRC-сканеры);

• программы-блокировщики;

• программы-иммунизаторы.

Программы-фаги (сканеры) используют для обнаружения вирусов метод сравнения с эталоном, метод эвристического анализа и некоторые другие методы. Программы-фаги осуществляют поиск характерной для конкретного вируса маски путем сканирования в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Программы-фаги не только находят зараженные вирусами файлы, но и «лечат» их, т. е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале работы программы-фаги сканируют оперативную память, обнаруживают вирусы и уничтожают их и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги — программы-фаги, предназначенные для поиска и уничтожения большого числа вирусов.

Программы-фаги можно разделить на две категории — универсальные и специализированные сканеры. Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от ОС, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов. Специализированные сканеры, рассчитанные только на макровирусы, оказываются более удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Программы-фаги делятся также на резидентные мониторы, производящие сканирование «на лету», и нерезидентные сканеры, обеспечивающие проверку системы только по запросу. Резидентные мониторы обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как нерезидентный сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам программ-фагов всех типов относится их универсальность. К недостаткам следует отнести относительно небольшую скорость поиска вирусов и относительно большие размеры антивирусных баз.

Программы-ревизоры (CRC-сканеры) используют для поиска вирусов метод обнаружения изменений. Принцип работы CRC-скане-ров основан на подсчете CRC-сумм (кодов циклического контроля) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) затем сохраняются в БД антивируса. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в БД, с реально подсчитанными значениями. Если информация о файле, записанная в БД, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. Как правило, сравнение состояний производят сразу после загрузки ОС.

CRC-сканеры, использующие алгоритмы анти-стеле, являются довольно мощным средством против вирусов: практически 100 % вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у CRC-сканеров имеется недостаток, заметно снижающий их эффективность: они не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их БД отсутствует информация об этих файлах.

Программы-блокировщики реализуют метод антивирусного мониторинга. Антивирусные блокировщики — это резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие об этом пользователю. К «вирусо-опасным» ситуациям относятся вызовы, которые характерны для вирусов в моменты их размножения (вызовы на открытие для записи в выполняемые файлы, запись в загрузочные секторы дисков или MBR винчестера, попытки программ остаться резидентно и т. п.).

При попытке какой-либо программы произвести указанные действия блокировщик посылает пользователю сообщение и предлагает запретить соответствующее действие. К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что бывает особенно полезно в случаях, когда регулярно появляется давно известный вирус. Однако они не «лечат» файлы и диски. Для уничтожения вирусов требуется применять другие программы, например фаги. К недостаткам блокировщиков можно отнести существование путей обхода их защиты и их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла).

Следует отметить, что созданы антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера. Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера.

Программы-иммунизаторы — это программы, предотвращающие заражение файлов. Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммуниза-торы, блокирующие заражение каким-либо типом вируса. Им-мунизаторы первого типа обычно записываются в конец файлов и при запуске файла каждый раз проверяют его на изменение. У таких иммунизаторов имеется один серьезный недостаток — они не могут обнаружить заражение стелс-виру-сом. Поэтому этот тип иммунизаторов практически не используются в настоящее время.

Иммунизатор второго типа защищает систему от поражения вирусом определенного вида. Он модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, вирус при этом воспринимает их зараженными и поэтому не внедряется. Такой тип иммунизации не может быть универсальным, поскольку нельзя иммунизировать файлы от всех известных вирусов. Однако в качестве полумеры подобные иммунизаторы могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет определяться антивирусными сканерами.

Профилактические меры защиты

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры. Абсолютно надежных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Важным методом борьбы с компьютерными вирусами является своевременная профилактика. Чтобы существенно уменьшить вероятность заражения вирусом и обеспечить надежное хранение информации на дисках, необходимо выполнять следующие меры профилактики:

• применять только лицензионное ПО;

• оснастить компьютер современными антивирусными программами и постоянно возобновлять их версии;

• всегда проверять съемные носители на наличие вирусов (запуская антивирусные программы своего компьютера) перед считыванием с них информации, записанной на других компьютерах;

• при переносе на свой компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

• периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив ОС с защищенной от записи системной дискеты;

• всегда защищать свои съемные носители от записи при работе на других компьютерах, если на них не будет производиться запись информации;

• обязательно делать на съемные носители архивные копии ценной для пользователя информации;

• использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей.

4.3. Сетевая защита

Межсетевой экран

Говоря о программно-аппаратной составляющей системы информационной безопасности, следует признать, что наиболее эффективный способ защиты объектов локальной сети (сегмента сети) от воздействий из открытых сетей (например, Интернета), предполагает размещение некоего элемента, осуществляющего контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Такой элемент получил название межсетевой экран (сетевой экран) или файрволл, брандмауэр.

Файрволл, файрвол, файервол, фаервол – образовано транслитерацией английского термина firewall.

Брандмауэр (нем. Brandmauer) – заимствованный из немецкого языка термин, являющийся аналогом английского "firewall" в его оригинальном значении (стена, которая разделяет смежные здания, предохраняя от распространения пожара).

Сетевой/межсетевой экран (МСЭ) – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов по различным протоколам в соответствии с заданными правилами.

Основной задачей межсетевого экрана является защита компьютерных сетей и/или отдельных узлов от несанкционированного доступа. Иногда межсетевые экраны называют фильтрами, так как их основная задача – не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Для того чтобы эффективно обеспечивать безопасность сети, межсетевой экран отслеживает и управляет всем потоком данных, проходящим через него. Для принятия управляющих решений для TCP/IP-сервисов (то есть передавать, блокировать или отмечать в журнале попытки установления соединений) межсетевой экран должен получать, запоминать, выбирать и обрабатывать информацию, полученную от всех коммуникационных уровней и от других приложений.

Межсетевой экран пропускает через себя весь трафик, принимая относительно каждого проходящего пакета решение: дать ему возможность пройти или нет. Для того чтобы межсетевой экран мог осуществить эту операцию, ему необходимо определить набор правил фильтрации. Решение о том, фильтровать ли с помощью межсетевого экрана пакеты данных, связанные с конкретными протоколами и адресами, зависит от принятой в защищаемой сети политики безопасности. По сути, межсетевой экран представляет собой набор компонентов, настраиваемых для реализации выбранной политики безопасности. Политика сетевой безопасности каждой организации должна включать (кроме всего прочего) две составляющие: политика доступа к сетевым сервисам и политика реализации межсетевых экранов.

Однако недостаточно просто проверять пакеты по отдельности. Информация о состоянии соединения, полученная из инспекции соединений в прошлом и других приложений – главный фактор в принятии управляющего решения при попытке установления нового соединения. Для принятия решения могут учитываться как состояние соединения (полученное из прошлого потока данных), так и состояние приложения (полученное из других приложений).

Таким образом, управляющие решения требуют, чтобы межсетевой экран имел доступ, возможность анализа и использования следующих факторов:

информации о соединениях – информация от всех семи уровней (модели OSI) в пакете;

истории соединений – информация, полученная от предыдущих соединений;

состоянии уровня приложения – информация о состоянии соединения, полученная из других приложений;

манипулировании информацией – вычисление разнообразных выражений, основанных на всех вышеперечисленных факторах.

Типы межсетевых экранов

Различают несколько типов межсетевых экранов в зависимости от следующих характеристик:

обеспечивает ли экран соединение между одним узлом и сетью или между двумя или более различными сетями;

происходит ли контроль потока данных на сетевом уровне или более высоких уровнях модели OSI;

отслеживаются ли состояния активных соединений или нет.

В зависимости от охвата контролируемых потоков данных межсетевые экраны подразделяются на:

традиционный сетевой (или межсетевой) экран – программа (или неотъемлемая часть операционной системы) на шлюзе (устройстве, передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями (объектами распределённой сети);

персональный межсетевой экран – программа, установленная на пользова-тельском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

В зависимости от уровня OSI, на котором происходит контроль доступа, сетевые экраны могут работать на:

сетевом уровне, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором;

сеансовом уровне (также известные, как stateful), когда отслеживаются сеансы между приложениями и не пропускаются пакеты, нарушающие спецификации TCP/IP, часто используемые в злонамеренных операциях – сканирование ресурсов, взломы через неправильные реализации TCP/IP, обрыв/замедление соединений, инъекция данных;

прикладном уровне (или уровне приложений), когда фильтрация производится на основании анализа данных приложения, передаваемых внутри пакета. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек.

Фильтрация на сетевом уровне

Фильтрация входящих и исходящих пакетов осуществляется на основе информации, содержащейся в следующих полях TCP- и IP-заголовков пакетов: IP-адрес отправителя; IP-адрес получателя; порт отправителя; порт получателя.

Фильтрация может быть реализована различными способами для блокирования соединений с определенными компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех компьютеров и сетей, которые считаются ненадежными.

К преимуществам такой фильтрации относится:

- сравнительно невысокая стоимость;

- гибкость в определении правил фильтрации;
- небольшая задержка при прохождении пакетов.

Недостатки:

- не собирает фрагментированные пакеты;
- нет возможности отслеживать взаимосвязи (соединения) между пакетами.

Фильтрация на сеансовом уровне

В зависимости от отслеживания активных соединений межсетевые экраны могут быть:

stateless (простая фильтрация), которые не отслеживают текущие соединения (например, TCP), а фильтруют поток данных исключительно на основе статических правил;

stateful, stateful packet inspection (SPI) (фильтрация с учётом контекста), с отслеживанием текущих соединений и пропуском только таких пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений.

Межсетевые экраны с SPI позволяют эффективнее бороться с различными видами DoS-атак и уязвимостями некоторых сетевых протоколов. Кроме того, они обеспечивают функционирование таких протоколов, как H.323, SIP, FTP и т. п., которые используют сложные схемы передачи данных между адресатами, плохо поддающиеся описанию статическими правилами, и зачастую несовместимых со стандартными, stateless сетевыми экранами.

К преимуществам такой фильтрации относится:

- анализ содержимого пакетов;
- не требуется информации о работе протоколов 7 уровня.

Недостатки:

- сложно анализировать данные уровня приложений (возможно с использованием ALG – Application level gateway).

Application level gateway, ALG (шлюз прикладного уровня) – компонент NAT-маршрутизатора, который понимает какой-либо прикладной протокол, и при прохождении через него пакетов этого протокола модифицирует их таким образом, что находящиеся за NAT’ом пользователи могут пользоваться протоколом.

Служба ALG обеспечивает поддержку протоколов на уровне приложений (таких как SIP, H.323, FTP и др.), для которых подмена адресов/портов (Network Address Translation) недопустима. Данная служба определяет тип приложения в пакетах, приходящих со стороны интерфейса внутренней сети и соответствующим образом выполняя для них трансляцию адресов/портов через внешний интерфейс.

Технология SPI (Stateful Packet Inspection) или технология инспекции пакетов с учетом состояния протокола на сегодня является передовым методом контроля трафика. Эта технология позволяет контролировать данные вплоть до уровня приложения, не требуя при этом отдельного приложения посредника или proxy для каждого защищаемого протокола или сетевой службы.

Исторически эволюция межсетевых экранов происходила от пакетных фильтров общего назначения, затем стали появляться программы-посредники для отдельных протоколов, и, наконец, была разработана технология stateful inspection. Предшествующие технологии только дополняли друг друга, но всеобъемлющего контроля за соединениями не обеспечивали. Пакетным фильтрам недоступна информация о состоянии соединения и приложения, которая необходима для принятия заключительного решения системой безопасности. Программы-посредники обрабатывают только данные уровня приложения, что зачастую порождает различные возможности для взлома системы. Архитектура stateful inspection уникальна потому, что она позволяет оперировать всей возможной информацией, проходящей через машину-шлюз: данными из пакета, данными о состоянии соединения, данными, необходимыми для приложения.

Пример работы механизма Stateful Inspection. Межсетевой экран отслеживает сессию FTP, проверяя данные на уровне приложения. Когда клиент запрашивает сервер об открытии обратного соединения (команда FTP PORT), межсетевой экран извлекает номер порта из этого запроса. В списке запоминаются адреса клиента и сервера, номера портов. При фиксировании попытки установить соединение FTP-data, межсетевой экран просматривает список и проверяет, действительно ли данное соединение является ответом на допустимый запрос клиента. Список соединений поддерживается динамически, так что открыты только необходимые порты FTP. Как только сессия закрывается, порты блокируются, обеспечивая высокий уровень защищенности.

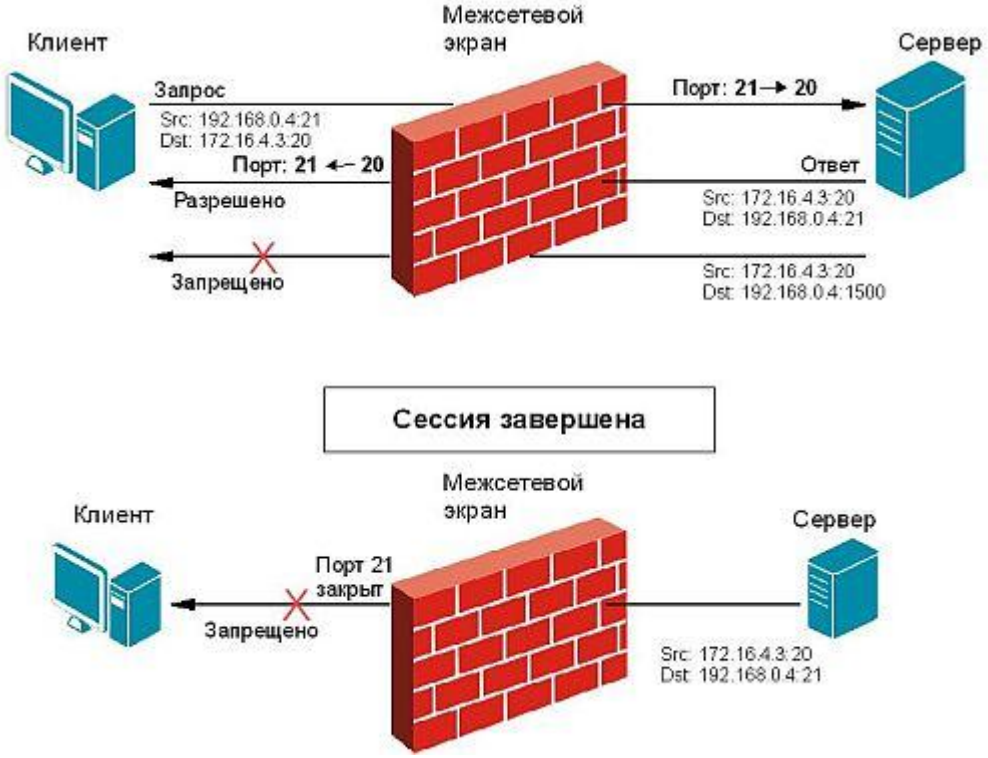

Рис. 4.2.1 Пример работы механизма Stateful Inspection с FTP-протоколом

Фильтрация на прикладном уровне

С целью защиты ряда уязвимых мест, присущих фильтрации пакетов, межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, как, например, Telnet, HTTP, FTP. Подобное приложение называется proxy-службой , а хост, на котором работает proxy-служба – шлюзом уровня приложений. Такой шлюз исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне (уровне приложений – верхний уровень сетевой модели) и может анализировать содержимое данных, например, адрес URL, содержащийся в HTTP-сообщении, или команду, содержащуюся в FTP-сообщении. Иногда эффективнее бывает фильтрация пакетов, основанная на информации, содержащейся в самих данных. Фильтры пакетов и фильтры уровня канала не используют содержимое информационного потока при принятии решений о фильтрации, но это можно сделать с помощью фильтрации уровня приложений. Фильтры уровня прил ожений могут использовать информацию из заголовка пакета, а также содержимого данных и информации о пользователе. Администраторы могут использовать фильтрацию уровня приложений для контроля доступа на основе идентичности пользователя и/или на основе конкретной задачи, которую пытается осуществить пользователь. В фильтрах уровня приложений можно установить правила на основе отдаваемых приложением команд. Например, администратор может запретить конкретному пользователю скачивать файлы на конкретный компьютер с помощью FTP или разрешить пользователю размещать файлы через FTP на том же самом компьютере.

К преимуществам такой фильтрации относится:

- простые правила фильтрации;
- возможность организации большого числа проверок. Защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, что снижает вероятность взлома с использованием "дыр" в программном обеспечении;
- способность анализировать данные приложений.

Недостатки:

- относительно низкая производительность по сравнению с фильтрацией пакетов;
- proxy должен понимать свой протокол (невозможность использования с неизвестными протоколами)?;
- как правило, работает под управлением сложных ОС.

Межсетевой экран не является симметричным устройством. Он различает понятия: "снаружи" и "внутри". Межсетевой экран обеспечивает защиту внутренней области от неконтролируемой и потенциально враждебной внешней среды. В то же время межсетевой экран позволяет разграничить доступ к объектам общедоступной сети со стороны субъектов защищенной сети. При нарушении полномочий работа субъекта доступа блокируется, и вся необходимая информация записывается в журнал.

Межсетевые экраны могут использоваться и внутри защищенных корпоративных сетей. Если в локальной сети имеются подсети с различной

степенью конфиденциальности информации, то такие фрагменты целесообразно отделять межсетевыми экранами. В этом случае экраны называют внутренними.

Прокси-сервер

Прокси-сервер (proxy – представитель, уполномоченный) – служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (cache) (в случаях, если прокси имеет свой кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента.

Proxy являются попыткой реализовать межсетевой экран на уровне приложения. Их основное преимущество – поддержка полной информации о приложениях. Proxy обеспечивают частичную информацию об истории соединений, полную информацию о приложении и частичную информацию о текущем соединении и имеют возможность обработки и действий над информацией.

Однако имеются очевидные трудности в использовании proxy на уровне приложения в качестве межсетевого экрана:

Ограничения на соединения – каждый сервис требует наличия своего собственного прокси, поэтому число доступных сервисов и их масштабируемость ограничены.

Ограничения технологии – шлюз прикладного уровня (ALG) не может обеспечить прокси для протокола UDP.

Производительность – реализация на уровне приложения имеет значительные потери в производительности.

В добавление, proxy беззащитны к ошибкам в приложениях и ОС, неверной информации в нижних уровнях протоколов и в случае традиционных прокси-серверы очень редко являются прозрачными.

Исторически proxy уровня приложений удовлетворяли общему их применению и нуждам сети Интернет. Однако, по мере превращения Интернета в постоянно меняющуюся динамичную среду, предлагающую новые протоколы, сервисы и приложения, proxy более не способны обработать различные типы взаимодействий в сети Интернет или отвечать новым нуждам бизнеса, высоким требованиям к пропускной способности и безопасности сетей.

Интернет-маршрутизатор

Так называемые классические маршрутизаторы действуют на сетевом уровне, и их очевидным недостатком является неспособность обеспечивать безопасность даже для наиболее известных сервисов и протоколов.

Маршрутизаторы не являются устройствами обеспечения безопасности, так как они не имеют основных возможностей межсетевого экрана:

информации о соединении – маршрутизаторы имеют доступ лишь к ограниченной части заголовка пакетов;

наследуемой информации о соединении и приложении – маршрутизаторы не поддерживают хранение информации об истории соединения или приложения;

манипулирований информацией – маршрутизаторы имеют очень ограниченные возможности по действиям над информацией.

К тому же, маршрутизаторы достаточно сложно конфигурировать, следить за их состоянием и управлять. Они не обеспечивают должного уровня журналирования событий и механизмов оповещения.

Интернет-маршрутизатор – это аппаратное решение с одним (или несколькими) портом WAN для подключения к сети общего пользования (Интернет) и несколькими (чаще четыре) портами LAN для подключения рабочих станций локальной сети. Иногда Интернет-маршрутизатор оборудован беспроводной точкой доступа для организации связи в локальной сети с беспроводными клиентами. Может оснащаться USB-портом для подключения принтера и/или других устройств (например, 3G-модема).

Интернет-маршрутизатор разработан для совместного доступа группы пользователей к широкополосному Интернет-соединению через выделенную линию, DSL или кабельный модем. Кроме того, в качестве дополнительного канала возможно применение 4G-модемов, обеспечивающих доступ в Интернет через 4G-сети.

Интернет-маршрутизатор оснащен встроенным межсетевым экраном для защиты компьютеров в сети от вирусных и DoS-атак. Управление доступом осуществляется с помощью фильтрации пакетов на основе MAC-адресов источника и приемника.

Маршрутизатор может быть настроен таким образом, что отдельные FTP, Web- и игровые серверы смогут совместно использовать один, видимый извне IP-адрес, и в тоже время останутся защищенными от атак хакеров. Пользователи через Web-интерфейс маршрутизатора могут настроить любой (или конкретно выделенный производителем для этой цели) из LAN-портов как DMZ-порт (см. раздел "Механизмы PAT и NAT"). В последнее время всё чаще стала присутствовать функция "родительского" контроля (Parental control), которая позволяет фильтровать нежелательные URL-адреса Web-сайтов, блокировать домены и управлять использованием Интернет по расписанию.

Поддержка Интернет-маршрутизаторами технологии QoS (см. раздел "Качество обслуживания (QoS) и управление полосой пропускания трафика (Traffic Shaping)") обеспечивает более эффективную передачу приложений, чувствительных к задержкам, таких как Интернет-телефония (VoIP), мультимедиа и игры по Интернет.

Таблица 4.3.1. Стандартный набор возможностей Интернет-маршрутизаторов и используемых в работе технологий

Типы подключения WAN:	Поддержка VPN:
Static IP Dynamic IP PPPoE L2TP PPTP DualAccess PPPoE DualAccess PPTP	PPTP pass-through IPSec pass-through L2TP pass-through

Функции Интернет-шлюза:

- Преобразование сетевых адресов (NAT)
- DHCP-сервер (для автоматического назначения параметров IP)
- Управление доступом пользователей:
- Фильтрация MAC-адресов
- Фильтрация по расписанию
- Межсетевой экран:
- NAT (преобразование сетевых адресов) с VPN pass-through
- SPI (Stateful Packet Inspection)
- Фильтрация Web-сайтов с помощью фильтрации URL-адресов.
- Приоритизация VoIP-трафика и потоковых медиафайлов при приеме/передаче.
- Широковещательный поток IGMP (Internet Group Management Protocol)

Фильтрация трафика

При отсутствии гибкой фильтрации доступа к сети Интернет на долю ненужных и опасных сайтов, ежедневно посещаемых сотрудниками, приходится чуть ли не половина общего трафика.

Лидерами в списке нежелательных ресурсов являются социальные сети, порталы, выкладывающие контент непристойного содержания, серверы онлайновых игр, а также сайты, генерирующие так называемый "тяжелый" трафик и предлагающие посетителям загружать и просматривать видеоролики и флэш-баннеры.

Потенциальные угрозы, возникающие в результате посещения сотрудниками различных не относящихся к выполняемой ими работе сайтов, помимо нецелевого использования рабочего времени, могут выглядеть как:

- чрезмерная нагрузка на сеть, вызванная неконтролируемым скачиванием сотрудниками объемных файлов из Интернет-сети. В случае, когда речь идет о постоянном или выделенном подключении с фиксированной скоростью канала от провайдера, просмотр или загрузка пользователями видеофайлов негативно скажется на распределении ресурсов сети и загрузке Интернет-канала в целом, а также на стоимости нецелевого трафика;

- нерациональное использование ресурсов сети и рабочего времени в результате деятельности любителей онлайновых игр с видео- или голосовыми чатами;
- неконтролируемые удаленные соединения сотрудников с рабочими серверами корпоративных сетей посредством VPN-соединений или утилит, связанные с риском заражения локальной сети вирусами, потенциально находящимися на удаленном компьютере;
- снижение уровня безопасности корпоративной сети.

Чтобы обеспечить безопасность и целостность бизнеса, перекрыть каналы возможной утечки информации и повысить производительность работы сотрудников, необходимо управлять потоком Интернет-трафика, входящего в локальную сеть при помощи фильтрации Интернет-запросов. Запрещая при помощи настройки фильтров доступ к тем или иным ресурсам, можно решить вопросы снижения затрат на нецелевые Интернет-ресурсы, а также значительно уменьшить риск инфицирования внутренних ресурсов корпоративной сети.

Виртуальные частные сети (VPN)

Интернет все чаще используется в качестве средства коммуникации между компьютерами, поскольку он предлагает эффективную и недорогую связь. Однако Интернет является сетью общего пользования и для того чтобы обеспечивать безопасную коммуникацию через него необходим некий механизм, удовлетворяющий как минимум следующим задачам:

- конфиденциальность информации;
- целостность данных;
- доступность информации;

Этим требованиям удовлетворяет механизм, названный VPN (Virtual Private Network – виртуальная частная сеть) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет) с использованием средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

Создание VPN не требует дополнительных инвестиций и позволяет отказаться от использования выделенных линий. В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: хост-хост, хост-сеть и сеть-сеть.

В решениях VPN используются такие средства, как шифрование данных для обеспечения целостности и конфиденциальности, аутентификация и авторизация для проверки прав пользователя и разрешения доступа к виртуальной частной сети.

VPN-соединение всегда состоит из канала типа точка-точка, также известного под названием туннель. Туннель создаётся в незащищённой сети, в качестве которой чаще всего выступает Интернет.

Туннелирование (tunneling) или инкапсуляция (encapsulation) – это способ передачи полезной информации через промежуточную сеть. Такой

информацией могут быть кадры (или пакеты) другого протокола. При инкапсуляции кадр не передается в том виде, в котором он был сгенерирован хостом-отправителем, а снабжается дополнительным заголовком, содержащим информацию о маршруте, позволяющую инкапсулированным пакетам проходить через промежуточную сеть (Интернет). На конце туннеля кадры деинкапсулируются и передаются получателю. Как правило, туннель создается двумя пограничными устройствами, размещенными в точках входа в публичную сеть. Одним из явных достоинств туннелирования является то, что данная технология позволяет зашифровать исходный пакет целиком, включая заголовок, в котором могут находиться данные, содержащие информацию, которую злоумышленники используют для взлома сети (например, IP-адреса, количество подсетей и т.д.).

Хотя VPN-туннель устанавливается между двумя точками, каждый узел может устанавливать дополнительные туннели с другими узлами. Для примера, когда трём удалённым станциям необходимо связаться с одним и тем же офисом, будет создано три отдельных VPN-туннеля к этому офису. Для всех туннелей узел на стороне офиса может быть одним и тем же.

Пользователь устанавливает соединение с VPN-шлюзом, после чего пользователю открывается доступ к внутренней сети.

Внутри частной сети самого шифрования не происходит. Причина в том, что эта часть сети считается безопасной и находящейся под непосредственным контролем в противоположность Интернету. Это справедливо и при соединении офисов с помощью VPN-шлюзов. Таким образом, гарантируется шифрование только той информации, которая передаётся по небезопасному каналу между офисами.

Существует множество различных решений для построения виртуальных частных сетей. Наиболее известные и широко используемые протоколы – это:

PPTP (Point-to-Point Tunneling Protocol) – этот протокол стал достаточно популярен благодаря его включению в операционные системы фирмы Microsoft.

L2TP (Layer-2 Tunneling Protocol) – сочетает в себе протокол L2F (Layer 2 Forwarding) и протокол PPTP. Как правило, используется в паре с IPSec.

IPSec(Internet Protocol Security) – официальный Интернет-стандарт, разработан сообществом IETF (Internet Engineering Task Force).

Система обнаружения и предотвращения атак (IDP)

Широко распространённые системы обнаружения вторжений IDS (Intrusion Detection System), используемые в межсетевых экранах, предназначены для обеспечения сетевого мониторинга, анализа и оповещения в случае обнаружения сетевой атаки. Как правило, механизм IDS основан на определённом шаблоне и выдаст сигнал тревоги в случае обнаружения необычного или атакующего трафика. Важно заметить, что системы подобные IDS не в состоянии остановить атаку, они лишь оповещают о ней.

Система предотвращения вторжений IPS (Intrusion Prevention Service) является системой сетевой профилактики нового поколения. Помимо

возможностей IDS, в этой системе обеспечивается возможность блокировать или отбрасывать нежелательные пакеты. Тем самым предохраняя внутренние узлы информационной системы от действий вредоносного трафика.

Обнаружение вторжений (Intrusion Detection)

Отличие вторжений от вирусных атак состоит в том, что вирус обычно содержится в отдельном загрузочном файле, который закачивается в систему пользователя, а вторжения проявляются, как образцы (шаблоны) вируса, нацеленные на поиск путей преодоления механизмов обеспечения безопасности. Такие угрозы встречаются довольно часто и постоянно развиваются, так как их создание может быть автоматизировано.

Подсистема обнаружения и предотвращения Intrusion Detection and Prevention (IDP) разработана для защиты против попыток вторжения. Контролируя сетевой трафик, проходящий через межсетевой экран, IDP определяет образцы (шаблоны) вируса, указывающие на то, что предпринято вторжение. Обнаружив вторжение один раз, IDP нейтрализует все последующие вторжения этого типа и их источник (как саму атаку, так и ее источник).

Правила IDP (IDP Rules)

IDP-правила определяют, какой трафик или сервис нужно анализировать. Структура IDP-правил подобна структуре других политик безопасности, например, IP-правил. IDP-правила определяют соответствие заданного интерфейса/адреса источника/получателя с объектом сервиса/протоколов. С IDP-правилами можно связать объект расписание.

Каждое правило IDP позволяет производить настройки процесса нормализации HTTP. Выбираются те условия, которые должны быть приняты при обнаружении IDP-несовместимости в URI (Uniform Resource Identifier – унифицированный идентификатор ресурса), встроенном в принятом запросе HTTP.

Условия URI, которые может детектировать IDP:

- Invalid UTF8 – Поиск любых недостоверных символов UTF-8 в URI.
- Invalid hex encoding – Поиск недостоверной шестнадцатеричной последовательности.
- Double encoding – Поиск любой шестнадцатеричной последовательности, которая зашифрована другой шестнадцатеричной последовательностью.

Порядок обработки пакетов следующий:

Входящий пакет принимается межсетевым экраном и IDS выполняет обычную проверку. Если пакет является частью нового соединения, то он проверяется IP-правилами перед прохождением к IDP-модулю. Если же пакет – часть существующего соединения, то он проходит прямо к IDP-системе. Если пакет не является частью существующего соединения или отклонен набором IP-правил, то он отбрасывается.

Информация об источнике и получателе сравниваются с набором IDP-правил, установленных администратором. Если соответствие найдено, то пакет

проходит на следующий уровень обработки IDP-правилами – Pattern Matching. Если же соответствие с заданными IDP-правилами не найдено, тогда пакет принимается и IDP-система не предпринимает никаких дальнейших действий, а пакет проверяется набором IP-правил, таких как переадресация и запись в журнал.

Для правильной идентификации вторжения IDP использует профиль признаков или образцов (шаблонов), связанных с различными типами атак. Определенные образцы вирусов и атак, известные как сигнатуры, хранятся в базе данных локальной системы IDP и используются IDP-модулем при анализе трафика. Каждая IDP-сигнатура имеет свой уникальный номер.

Приведем пример простой атаки с использованием FTP-сервера. Злоумышленник может восстановить файл пароля "passwd" от FTP-сервера, используя FTP-команду RETR passwd. Сигнатура, ищущая ASCII-текст RETR и passwd, найдет соответствие и укажет на возможное вторжение. В рассмотренном примере образец найден в открытом тексте, также соответствие с образцом определяется и при использовании двоичных данных.

IDP предлагает три типа сигнатур, различающиеся уровнем защиты от угроз:

Сигнатуры предотвращения вторжений (IPS – Intrusion Protection Signatures) – сигнатуры с очень высокой точностью. Рекомендуется использование действия Protect. Эти сигнатуры могут обнаружить попытки перехвата управления и сканеры сети (типа Nmap).

Сигнатуры обнаружения вторжения (IDS – Intrusion Detection Signatures) – способны обнаруживать события, которые могут оказаться вторжениями. Эти сигнатур менее точны, чем IPS, поэтому перед действием Protect рекомендуется использовать действие Audit .

Политики сигнатур (Policy Signatures) – обнаруживают различные типы приложений трафика и могут использоваться для блокировки определенных приложений (например, совместный доступ к файлам или мгновенная передача сообщений).

4.4. Криптографические методы защиты информации

Криптографические методы защиты информации – это мощное оружие в борьбе за информационную безопасность.

Криптография (от древне-греч. κρυπτος – скрытый и γραφω – пишу) – наука о методах обеспечения конфиденциальности и аутентичности информации.

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

- защиту конфиденциальности;
- защиту целостности.

Проблемы защиты конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы обозначенные на рис 4.4.1:

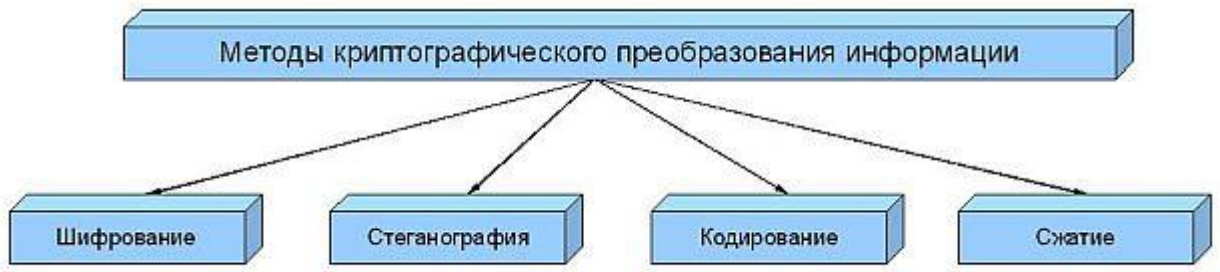

Рис. 4.4.1 Классификация методов криптографического преобразования информации.

Процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служит информация, подлежащая зашифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемых при реализации алгоритма шифрования. Операнд – это константа, переменная, функция, выражение и другой объект языка программирования, над которым производятся операции.

В отличие от других методов криптографического преобразования информации, методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов, т.е. скрываются секретные данные, при этом создаются реалистичные данные, которые невозможно отличить от настоящих. Обработка мультимедийных файлов в информационных системах открыла практически неограниченные возможности перед стеганографией.

Графическая и звуковая информация представляются в числовом виде. Так, в графических объектах наименьший элемент изображения может

кодироваться одним байтом. В младшие разряды определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение.

Скрытый файл также может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Содержанием процесса кодирование информации является замена исходного смысла сообщения (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, знаков. При кодировании и обратном преобразовании используются специальные таблицы или словари. В информационных сетях кодирование исходного сообщения (или сигнала) программно-аппаратными средствами применяется для повышения достоверности передаваемой информации.

Часто кодирование и шифрование ошибочно принимают за одно и тоже, забыв о том, что для восстановления закодированного сообщения, достаточно знать правило замены, в то время как для расшифровки сообщения помимо знания правил шифрования, требуется ключ к шифру.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени передачи данных целесообразно совмещать процесс сжатия и шифрования информации.

Основным видом криптографического преобразования информации в компьютерных сетях является шифрование. Под шифрованием понимается процесс преобразования открытой информации в зашифрованную информацию (шифртекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название зашифрование, а процесс преобразования закрытой информации в открытую – расшифрование.

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров. Методом шифрования (шифром) называется совокупность обратимых

преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, а некоторые используются и до сих пор. Появление компьютеров и компьютерных сетей инициировало процесс разработки новых шифров, учитывающих возможности использования компьютерной техники как для зашифрования/расшифрования информации, так и для атак на шифр. Атака на шифр (криптоанализ, криптоатака) – это процесс расшифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

Современные методы шифрования должны отвечать следующим требованиям:

- стойкость шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;
- криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
- шифртекст не должен существенно превосходить по объему исходную информацию;
- ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;
- время шифрования не должно быть большим;
- стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифртексту, при условии, что ему неизвестен ключ.

Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь скрытых слабых мест, которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации – перебор комбинаций ключа и выполнение алгоритма расшифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.

Работа простой криптосистемы проиллюстрирована на рис. 4.4.2

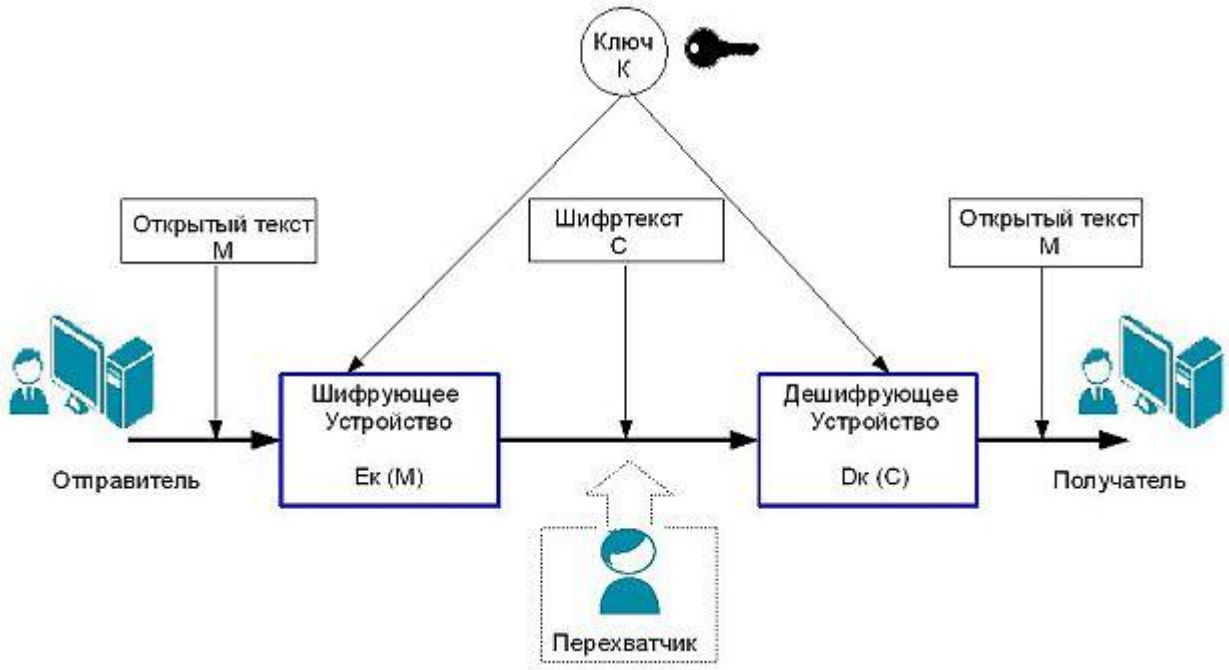

Рис. 4.4.2. Обобщённая схема криптографической системы

Отправитель генерирует открытый текст исходного сообщения М, которое должно быть передано законному получателю по незащищённому каналу. За каналом следит перехватчик с целью перехватить и раскрыть передаваемое сообщение. Для того чтобы перехватчик не смог узнать содержание сообщения М, отправитель шифрует его с помощью обратимого преобразования Ек и получает шифртекст (или криптограмму) С=Ек(М) , который отправляет получателю.

Законный получатель, приняв шифртекст С, расшифровывает его с помощью обратного преобразования Dк(С) и получает исходное сообщение в виде открытого текста М.

Преобразование Ек выбирается из семейства криптографических преобразований, называемых криптоалгоритмами. Параметр, с помощью которого выбирается отдельное преобразование, называется криптографическим ключом К.

Криптосистема имеет разные варианты реализации: набор инструкций, аппаратные средства, комплекс программ, которые позволяют зашифровать открытый текст и расшифровать шифртекст различными способами, один из которых выбирается с помощью конкретного ключа К.

Преобразование шифрования может быть симметричным и асимметричным относительно преобразования расшифрования. Это важное свойство определяет два класса криптосистем:

- симметричные (одноключевые) криптосистемы;
- асимметричные (двухключевые) криптосистемы (с открытым ключом).

Симметричное шифрование

Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, в основном используется для обеспечения

конфиденциальности данных. Для того чтобы обеспечить конфиденциальность данных, пользователи должны совместно выбрать единый математический алгоритм, который будет использоваться для шифрования и расшифровки данных. Кроме того, им нужно выбрать общий (секретный) ключ, который будет использоваться с принятым ими алгоритмом шифрования/дешифрования, т.е. один и тот же ключ используется и для зашифрования, и для расшифрования (слово "симметричный" означает одинаковый для обеих сторон).

Пример симметричного шифрования показан на рис. 2.2.

Сегодня широко используются такие алгоритмы шифрования, как Data Encryption Standard (DES), 3DES (или "тройной DES") и International Data Encryption Algorithm (IDEA). Эти алгоритмы шифруют сообщения блоками по 64 бита. Если объем сообщения превышает 64 бита (как это обычно и бывает), необходимо разбить его на блоки по 64 бита в каждом, а затем каким-то образом свести их воедино. Такое объединение, как правило, происходит одним из следующих четырех методов:

- электронной кодовой книги (Electronic Code Book, ECB);
- цепочки зашифрованных блоков (Cipher Block Changing, CBC);
- x-битовой зашифрованной обратной связи (Cipher FeedBack, CFB-x);
- выходной обратной связи (Output FeedBack, OFB).

Triple DES (3DES) – симметричный блочный шифр, созданный на основе алгоритма DES, с целью устранения главного недостатка последнего – малой длины ключа (56 бит), который может быть взломан методом полного перебора ключа. Скорость работы 3DES в 3 раза ниже, чем у DES, но криптостойкость намного выше. Время, требуемое для криптоанализа 3DES, может быть намного больше, чем время, нужное для вскрытия DES.

Алгоритм AES (Advanced Encryption Standard), также известный как Rijndael – симметричный алгоритм блочного шифрования – шифрует сообщения блоками по 128 бит, использует ключ 128/192/256 бит.

Шифрование с помощью секретного ключа часто используется для поддержки конфиденциальности данных и очень эффективно реализуется с помощью неизменяемых "вшитых" программ (firmware). Этот метод можно использовать для аутентификации и поддержания целостности данных.

С методом симметричного шифрования связаны следующие проблемы:

необходимо часто менять секретные ключи, поскольку всегда существует риск их случайного раскрытия (компрометации);

достаточно сложно обеспечить безопасность секретных ключей при их генерировании, распространении и хранении.

Асимметричное шифрование

Асимметричное шифрование часто называют шифрованием с помощью открытого ключа, при котором используются разные, но взаимно дополняющие друг друга ключи и алгоритмы шифрования и расшифровки. Отношение между ключами является математическим – один ключ зашифровывает информацию, а другой ее расшифровывает.

Асимметричное шифрование – система шифрования и/или электронной цифровой подписи (ЭЦП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу, и используется для проверки ЭЦП и для шифрования сообщения. Для генерации цифровой подписи и для расшифрования сообщения используется секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в защищенных протоколах передачи данных TLS и его предшественнике SSL (лежащих в основе протокола HTTPS), в протоколе безопасного удаленного управления SSH. Также используется в протоколах шифрования электронной почты PGP и S/MIME.

Для того чтобы установить связь с использованием шифрования через открытый ключ, обеим сторонам нужно получить два ключа: открытый К1 и частный (секретный) К2 (рис. 2.3). Для шифрования и расшифровки данных обе стороны будут пользоваться разными ключами.

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищённому схеме распространения ключей (например из рук в руки или с помощью поверенного курьера). В асимметричной криптосистеме по подобной схеме передается только открытый ключ, а частный (секретный) ключ хранится на месте его генерации (у владельца).

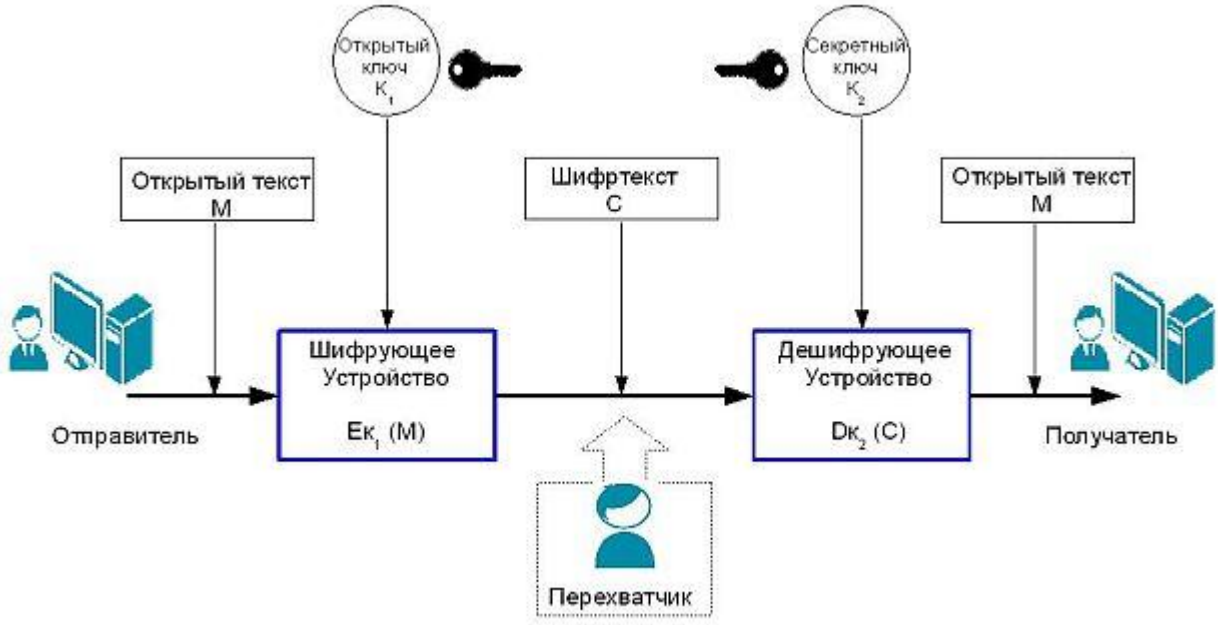

Рис. 4.4.3. Обобщенная схема асимметричной криптосистемы

Механизмы генерирования пар открытых/частных ключей являются достаточно сложными, но в результате получаются пары очень больших случайных чисел, одно из которых становится открытым ключом, а другое – секретным. Генерирование таких чисел требует больших процессорных мощностей, поскольку эти числа, а также их произведения должны отвечать строгим математическим критериям. Однако этот процесс генерирования абсолютно необходим для обеспечения уникальности каждой пары

открытых/частных ключей. Алгоритмы шифрования с использованием открытых ключей часто используют в приложениях, где аутентификация проводится с помощью цифровой подписи и управления ключами.

Среди наиболее известных алгоритмов открытых ключей можно назвать RSA (Rivest-Shamir-Adleman) и DSA (Digital Signature Algorithm). Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм DSA применяется для создания цифровой подписи, но не для шифрования

При использовании алгоритма RSA можно не только использовать открытый ключ для зашифрования, а секретный для расшифрования, но и наоборот: данные можно зашифровать с помощью секретного ключа, а открытый ключ применять при расшифровывании данных. Конечно, такой способ не дает возможность сохранять секреты, поскольку открытый ключ свободно доступен и любой может расшифровать информацию, но это дает способ поручиться за целостность содержимого сообщения: если открытый ключ правильно расшифровывает данные, значит, они были зашифрованы с помощью секретного ключа. Такой метод называется электронной цифровой подписью. Идея применения цифровой подписи строится на двух основных предположениях: во-первых, что секретный ключ уникален и защищен (только владелец ключа имеет к нему доступ), и, во-вторых, единственным способом поставить цифровую подпись является применение этого секретного ключа.

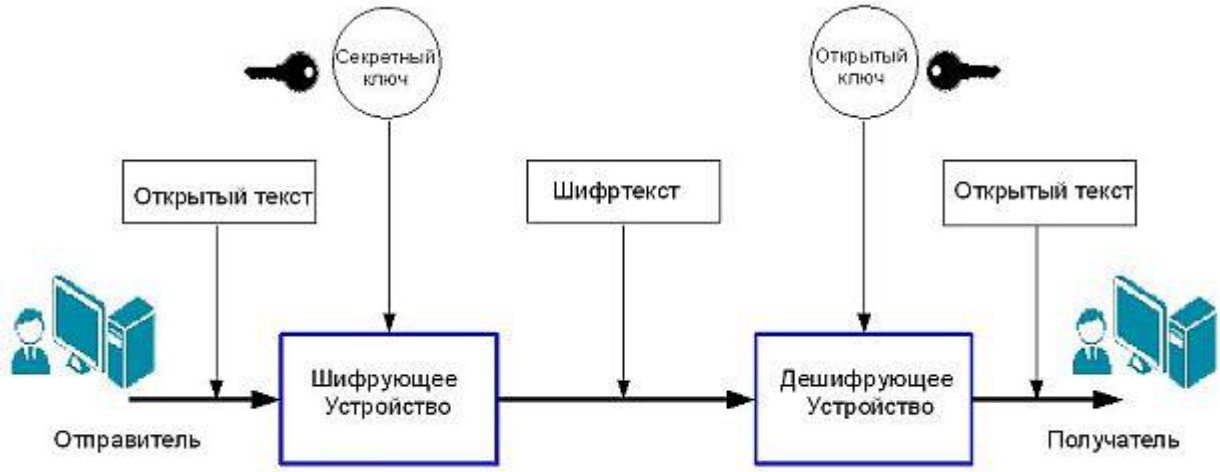

Рис. 4.4.4. Применение цифровой подписи

Если данные зашифрованы с помощью не секретного ключа отправителя, а, например, открытого ключа или какого-либо другого, то получатель, расшифровав данные с использованием открытого ключа, получит не открытый текст сообщения, а бессмыслицу.

Как правило, при создании цифровой подписи шифруется не весь открытый текст, а определенный фрагмент, так называемый дайджест сообщения (message digest), который генерируется (на основе вычислений) из исходного текста сообщения. К нему добавляется информация о том, кто подписывает документ. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного

алгоритма. Получившийся зашифрованный набор бит и представляет собой подпись.

Отправитель посылает дайджест сообщения вместе с этим сообщением. При приеме получателем производятся такие же вычисления дайджеста. Если в сообщение были внесены изменения, результат вычисления будет отличаться от полученного, что свидетельствует о том, что целостность сообщения нарушена.

Алгоритм вычисления дайджеста принимает входные данные любой длины и преобразует их, чтобы получить псевдослучайный результат фиксированной длины. Другой термин, часто использующийся для дайджеста сообщений, – это хэш.

Хэш (hash) – это результат преобразования входных данных произвольной длины в данные фиксированной длины. Функция, с помощью которой реализуется это преобразование, называется функция хэширования или хэш-функция.

В криптографии принято выделять криптографически стойкие хэш-функции, удовлетворяющие следующим условиям: во-первых, необратимость (т.е. невозможность восстановления исходного текста по результатам вычислений) и, во-вторых, стойкость к коллизиям. Коллизия – это ситуация, когда двум сообщениям соответствует один и тот же хэш. Наиболее часто в качестве алгоритма хэширования используется алгоритм MD5 (генерируется 128-битное значение) или SHA-1 (генерируется 160-битное значение).

Хэш-функции широко применяются при создании пользовательских паролей, когда строка произвольной длины (пароль) преобразуется в указанный ключ заранее заданной длины, и для проверки целостности данных, когда данные отправляются вместе с контрольным значением.

Сертификаты открытых ключей

Криптография с открытым ключом предоставляет не только мощный механизм для шифрования, но и средства идентификации и аутентификации пользователей и устройств. Однако, если между отправителем и получателем нет конфиденциальной схемы передачи асимметричных ключей, то возникает серьезная опасность появления злоумышленника-посредника. Ручное распространение ключей становится непрактичным и создает бреши в системе безопасности. По этим причинам было разработано другое решение – применение сертификатов открытых ключей.

В своей основной форме сертификатом называется информационный пакет, содержащий открытый ключ, электронную подпись, подтверждающую этот ключ, и имя доверенной третьей стороны, удостоверяющей достоверность этих фактов. Третья сторона, которой доверяют пользователи и которая подтверждает идентичность пользователя и его права, называется удостоверяющим центром CA (Certificate Authority) или центром сертификации . CA создает сертификаты пользователей, включающие следующую информацию: имя пользователя (сюда же относится пароль и другие дополнительные сведения, однозначно идентифицирующие этого

пользователя), открытый ключ пользователя, время действия сертификата, конкретные операции, в которых этот ключ может быть использован (идентификация, шифрование). Удостоверяющий центр полностью ответственен за аутентичность своих конечных пользователей.

Удостоверяющие центры можно разделить на 2 категории: открытые и частные. Открытые CA действуют через Интернет, предоставляя услуги сертификации всем желающим. Частные CA, как правило, принадлежат организациям или закрытым сетям и выдают сертификаты только пользователям локальных сетей.

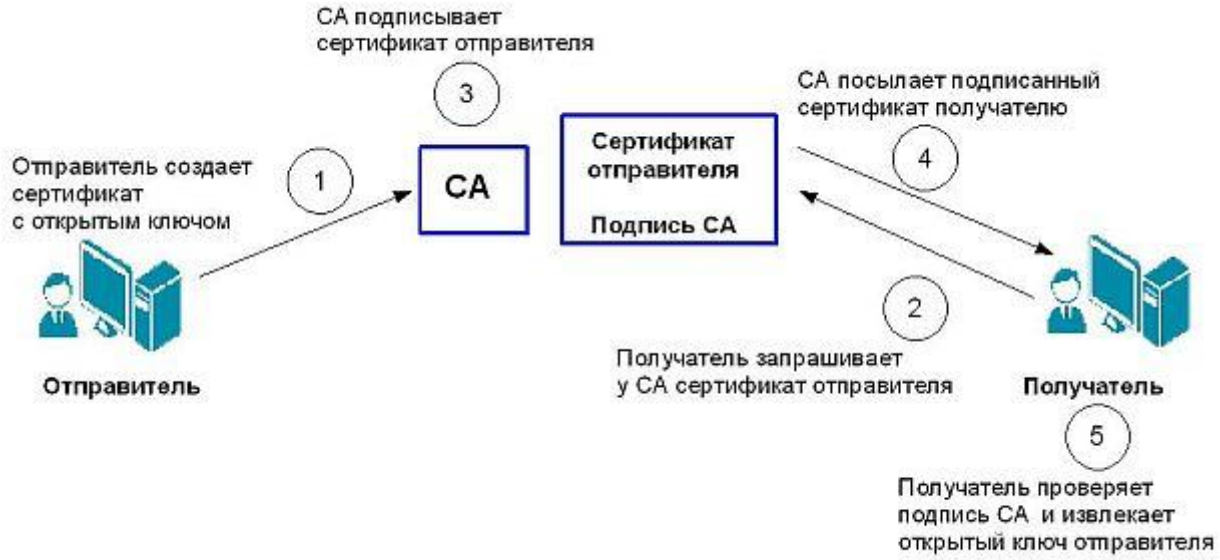

Рис. 4.4.5. Выдача сертификатов удостоверяющим центром CA

Наиболее широко распространенным форматом сертификатов, принятым для технологии открытых ключей, является стандарт X.509 v.3, описанный в документах RFC 2459 и RFC 5280.

Надежной системой распространения открытого ключа CA является инфраструктура открытых ключей PKI (Public Key Infrastructure), которая определяет взаимодействие между конечными пользователями и доверяющими сторонами, предоставляя возможность безопасно выпускать и работать с сертификатами.

4.5.Управления непрерывностью бизнеса

Управление непрерывностью бизнеса компании является циклическим процессом, который должен учитывать возможные изменения в бизнесе, сфере ИТ, законодательстве и других областях, влияющие на деятельность организации, а также помогать ей адаптироваться к этим изменениям. Другими словами, управление непрерывностью бизнеса является процессом его

постоянного совершенствования, что, в свою очередь, повышает уверенность компании в надежности планов обеспечения непрерывности бизнеса.

Жизненный цикл процесса управления непрерывностью бизнеса включает 7 этапов, на каждом из которых определены последовательность шагов и результат.

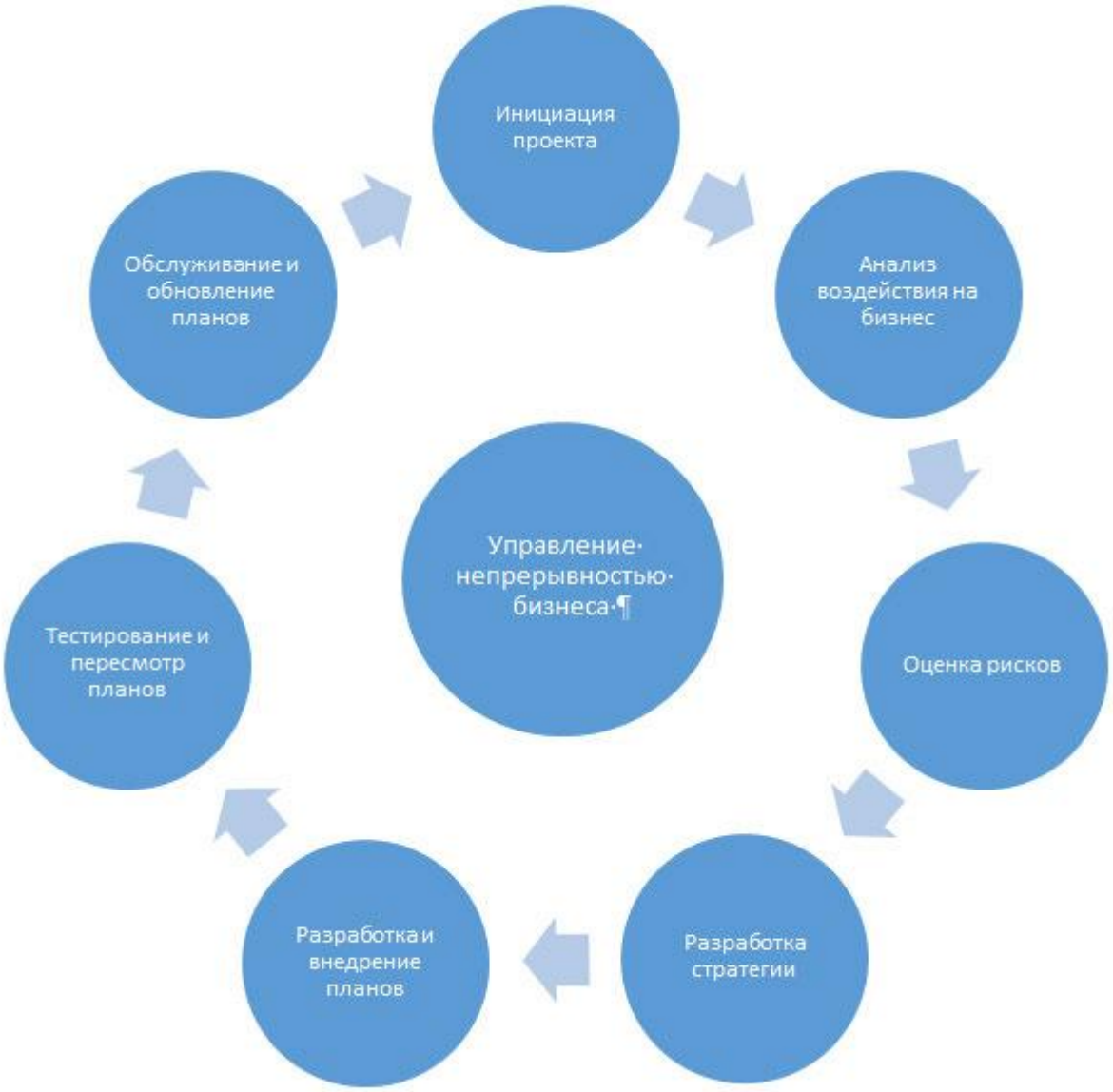

Рис. 4.5.1. Жизненный цикл процесса управления непрерывностью бизнеса

1. Инициация проекта

План управления проектом / Project Management Plan – документ, описывающий, как проект будет исполняться, как будет происходить его мониторинг и контроль. На данном этапе определяется содержание проекта обеспечения непрерывности бизнеса и разрабатывается его пошаговый план. В нем определяется, как будет исполняться проект, как будет проводиться его мониторинг, контроль и закрытие, а также определяются границы проекта, роли членов проектной команды и цели проекта.

Помимо вышеперечисленных действий, необходимо определить потребность в проекте. Для некоторых компаний непрерывность бизнеса — это обеспечение эффективности критически важных бизнес-функций, а также демонстрация устойчивости бизнеса клиентам. Но нельзя забывать, что существуют требования нормативно-правовых актов и регулирующих органов к непрерывности бизнеса. Далее в таблице 4.5.1 перечислены и описаны стандарты / нормативно-правовые акты (НПА) широко использующиеся на территории Российской Федерации, а также ряд требований, которые предъявляют данные стандарты / НПА к системе непрерывности бизнеса.

Таблица 4.5.1 Стандарты и нормативно-правовые акты (НПА) с требованиями непрерывности бизнеса

Стандарт/ НПА	Требование	Описание	Статус
ISO/IEC 27001:2013 «Information technology — Security techniques — Information security management systems — Requirements» (Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности)	A.17 Information security aspects of business continuity management (Аспекты информационной безопасности в управлении непрерывностью бизнеса)	Непрерывность информационной безопасности должна быть встроена в систему непрерывности бизнеса компании Для этого необходимо: - спланировать непрерывность информационной безопасности; — внедрить непрерывность информационной безопасности; — проверить, оценить непрерывность информационной безопасности.	Непрерывность информационной безопасности является одним из требований в том случае, если компания стремится получить сертификат соответствия требованиям ISO/IEC 27001:2013 «Information technology — Security techniques — Information security management systems —

			Requirements».
ISO 22301:2012 «Societal security — Business continuity management systems — Requirements» (Социальная безопасность. Системы менеджмента непрерывности бизнеса)	Данный стандарт посвящен непрерывности бизнеса.	В стандарте прописаны: — требования, необходимые для установления системы менеджмента непрерывности бизнеса в компании; — требования к функциям высшего руководства в системе менеджмента непрерывности бизнеса; — требования к установлению стратегических целей и руководящих принципов системы менеджмента непрерывности бизнеса; — требования к обеспечению непрерывности бизнеса, порядок разработки процедур управления в условиях инцидента.	Наличие планов BCP/DRP (данные планы рассмотрены в разделе «Разработка и внедрение планов») является обязательным условием в том случае, если компания стремится получить сертификат соответствия требованиям ISO 22301:2012 «Societal security — Business continuity management systems — Requirements».
ГОСТ Р 53647 «Менеджмент непрерывности бизнеса»	Данный стандарт посвящен непрерывности бизнеса.	Настоящий стандарт устанавливает требования к планированию, созданию, функционированию, мониторингу, анализу, проведению учений,	Носит рекомендательный характер.

		поддержке и улучшению документированной системы менеджмента непрерывности бизнеса.	
СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»	8.11. Требования к организации и обеспечения непрерывности бизнеса и его восстановления после прерываний	В организации банковской системы должен быть определен план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания. План должен содержать инструкции и порядок действий работников организации банковской системы по восстановлению бизнеса. В частности, в состав плана должны быть включены: — условия активации плана; — действия, которые должны быть предприняты после инцидента ИБ; — процедуры восстановления; — процедуры тестирования и проверки плана; - план обучения и повышения осведомленности сотрудников; - обязанности сотрудников с указанием ответственных за выполнение каждого из положений плана. Также должны быть установлены требования по обеспечению ИБ, регламентирующие вопросы обеспечения непрерывности бизнеса и	Носит рекомендательный характер.

		его восстановлению после прерывания, в том числе требования к мероприятиям по восстановлению необходимой информации, программного обеспечения, технических средств, а также каналов связи.	
Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»	X. Обеспечение доступности информации (ОДТ)	В соответствии с Приказом ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» необходимо: — использовать отказоустойчивые технические средства; — резервировать технические средства, программное обеспечения, каналы передачи информации, средства обеспечения функционирования информационной системы; — контролировать безотказное функционирование технических средств; — обеспечить обнаружение и локализацию отказов функционирования технических средств; — принимать меры по восстановлению	В случае если система классифицирована по 1 или 2 классу защищенности, описанные в приказе требования носят обязательный характер.

		отказавших средств; — тестировать технические средства; — осуществлять периодическое резервное копирование информации на резервные машинные носители; — обеспечить возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала; — контролировать состояние и качество предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации.	
Приказ ФСТЭК России от 18.02.2013 г.№ 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»	X. Обеспечение доступности персональных данных (ОДТ)	В соответствии с Приказом ФСТЭК России от 18.02.2013 г.№ 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» необходимо обеспечить: — контроль безотказного функционирования технических средств; - обнаружение и локализацию отказов функционирования; — принятие мер по	В том случае, если для информационной системы персональных данных определен 1 или 2 уровень защищенности, описанные в приказе требования носят обязательный характер.

		восстановлению отказавших средств и их тестирование; — резервное копирование персональных данных на резервные машинные носители персональных данных; — возможность восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала.	

После того, как план проекта окончательно сформирован и разработан, его необходимо направить руководству компании для утверждения. Работа по плану должна начинаться только после согласования с руководством. В некоторых компаниях спонсор проекта не уделяет ему должного внимания, и ответственность возлагается на менеджера среднего звена. Это может привести к проблемам в коммуникации заинтересованных сторон и снижению поддержки высшего руководства компании. Данную проблему можно решить путем создания проектного комитета, куда войдут представители всех заинтересованных сторон. Комитет должен периодически проводить встречи, решать проблемы и обсуждать ход проекта.

2. Анализ воздействия на бизнес

Анализ воздействия на бизнес — метод позволяющий исследовать воздействие инцидентов на ключевые виды деятельности и процессы компании.

На данном этапе предусмотрено детальное изучение процессов компании. Для этого консультант проводит интервью с руководством отделов, входящих в область проекта. В ходе беседы запрашивается информация о деятельности отдела и составляется перечень процессов / функций, которые он осуществляет. Далее для детального изучения процессов / функций, интервьюируются владельцы процессов и определяется тип воздействия на бизнес (материальный, репутационный) и степень зависимости процесса от ИТ и внешних сервисов. А затем определяется максимально допустимое время простоя (Maximum Allowable Outage).

Maximum Allowable Outage — период времени, по истечении которого существует угроза окончательной утраты жизнеспособности организации, в том случае, если поставка продукции и/или предоставление услуг не будут возобновлены.

После того как владельцем процесса / функции был определен МАО, ИТ-департаментом (на основе МАО) определяются показатели RTO, RPO, SDO.

- Recovery Time Objective (RTO). Время, в течение которого должно происходить восстановление бизнес-функции или ресурса при наступлении нештатных ситуаций.
- Recovery Point Objective (RPO). Целевая точка восстановления определяет объем допустимых потерь данных в случае прерывания операций. Например, если RPO равен 15 минутам – допускается потеря данных за последние 15 минут.
- Service Delivery Objective (SDO). Уровень доступности сервиса в определенный момент времени.

На рисунке 4.5.2 изображено, как определяются вышеперечисленные метрики.

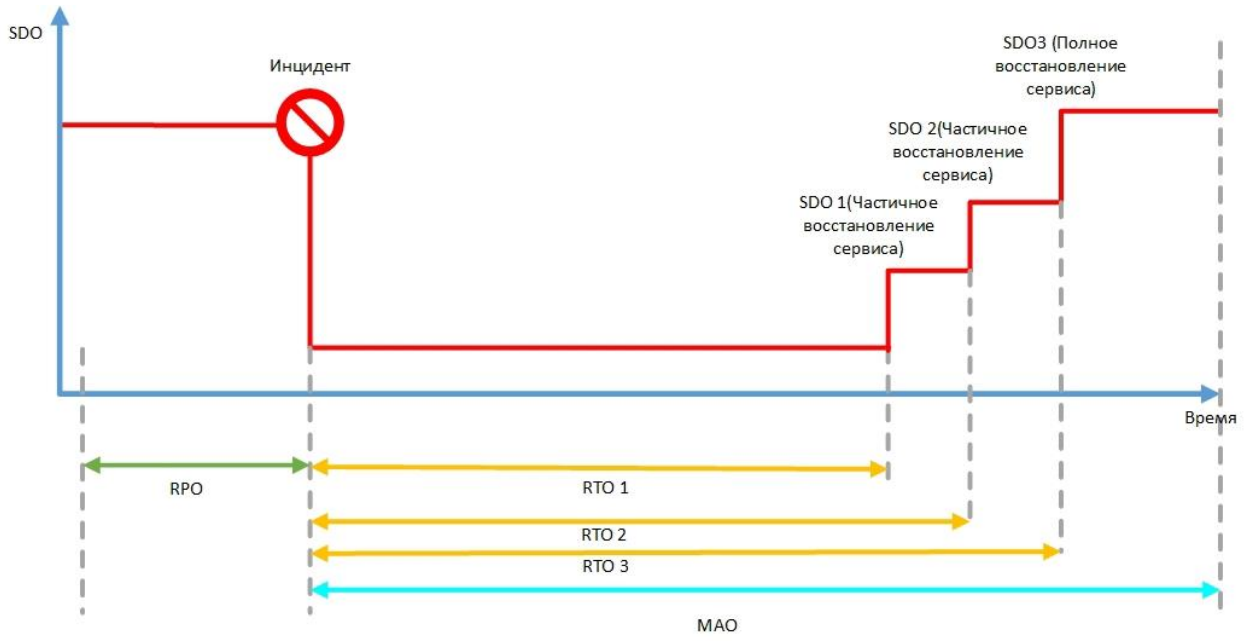

Рис. 4.5.2. График соотнешения метрик

Результатом проведения анализа воздействия на бизнес являются:

- перечень ранжированных по приоритетам критических процессов и соответствующих взаимозависимостей;
- зарегистрированные экономические и производственные воздействия, вызванные нарушением критических процессов;
- вспомогательные ресурсы, необходимые для идентифицированных критических процессов;
- возможные сроки простоя и восстановления критических процессов и взаимосвязанных информационных технологий.

Зачастую владельцы бизнес-процессов намеренно или неосознанно завышают целевые значение нормативов восстановления, что способствует искажению анализа и влечет за собой необоснованные расходы. Чтобы избежать этой проблемы, необходимо вместе с проектной группой, а также с заинтересованными сторонами рассмотреть ценность бизнес-функции в

контексте происшествия, которое затронуло всю компанию. Этот подход позволит объективно определить нормативы восстановления.

3. Оценка рисков

Риск — влияние неопределенности на цели.

Оценка риска / risk assessment — процесс, охватывающий идентификацию риска, анализ риска и оценку риска. ISO 73:2009 «Менеджмент рисков. Словарь». Целью оценки рисков в рамках управления непрерывностью бизнеса является определение событий, которые могут привести к нарушению деятельности компании, а также их последствий (ущерб). Оценка риска обеспечивает:

- понимание потенциальных опасностей и воздействия их последствий на достижение установленных целей компании;— понимание угроз и их источников;
- идентификацию ключевых факторов, формирующих риск; уязвимых мест компании и ее систем;
- выбор способов обработки риска;
- соответствие требованиям стандартов.

Процесс оценки рисков состоит из:

- Идентификации риска — процесс определения элементов риска, описания каждого из них, составления их перечня. Целью идентификации риска является составление перечня источников риска и угроз, которые могут повлиять на достижение каждой из установленных целей компании;
- Анализ риска — процесс исследования информации о риске. Анализ риска обеспечивает входные данные процесса общей оценки риска, помогает в принятии решений относительно необходимости обработки риска, а также в выборе соответствующей стратегии и методов обработки;
- Сравнительная оценка риска — сопоставление его уровня с критериями, установленными при определении области применения менеджмента риска, для определения типа риска и его значимости.

Оценка рисков в дальнейшем позволит обоснованно выработать стратегию непрерывности бизнеса, а также поможет определить оптимальный сценарий ее реализации.

4. Разработка стратегии непрерывности бизнеса

После того как были проанализировали требования к непрерывности, необходимо выбрать и обосновать возможные технические и организационные решения. В процессе выбора решения необходимо детально рассмотреть возможные действия в отношении помещений, технологий, информационных активов, контрагентов, а также партнеров. Данные решения, как правило, выбираются с целью:

- защиты приоритетных видов деятельности компании;

- их эффективного восстановления;
- смягчения последствий инцидентов, разработки ответных и превентивных мер.

Выбор решения должен основываться на стоимости восстановления и стоимости простоя.

Данные решения могут включать в себя:

- «Зеркальные» площадки;
- «Горячие» площадки;
- «Теплые» площадки;
- «Холодные» площадки;
- Площадки динамического распределения нагрузки;
- Аутсорсинг \ Соглашение;
- Мобильные площадки.

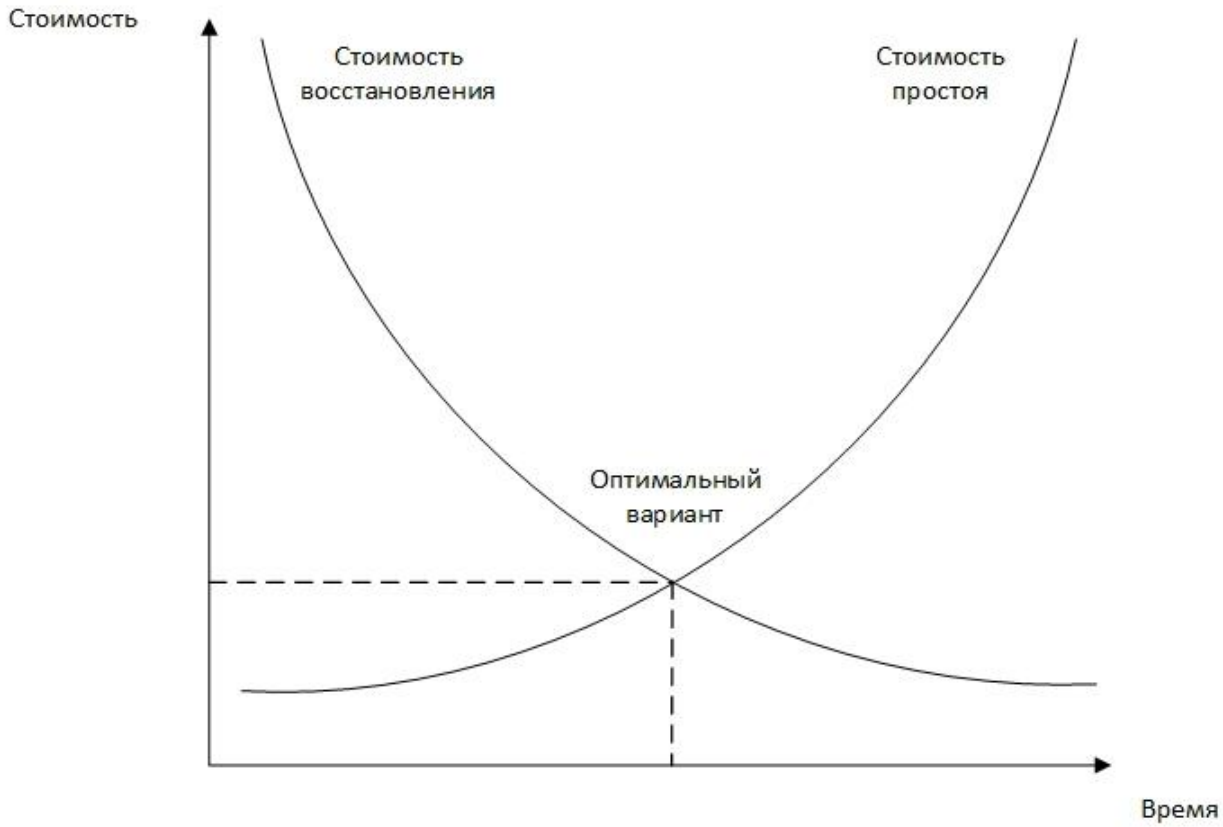

Рис. 4.5.3. График поиска оптимального варианта

Основными отличиями вышеперечисленных решений являются стоимость и время восстановления деятельности компании.

Решения помогают в реализации эффективной стратегии непрерывности бизнеса. Но для того, чтобы определить оптимальный вариант, необходимо выбирать стратегические решения, исходя из результатов анализа воздействий на бизнес и оценки рисков (этот подход поможет обосновать руководству необходимость инвестиций в проект управления непрерывностью бизнеса).

5. Разработка и внедрение планов непрерывности бизнеса

План – это заранее намеченная система мероприятий, предусматривающая порядок, последовательность и сроки выполнения работ.

В соответствии с лучшими практиками планы управления непрерывностью должны состоять из трёх компонентов:

1. Реагирование на чрезвычайные ситуации — определяет последовательность действий, которые необходимо осуществить при обнаружении инцидента.

2. Управление инцидентами — определяет методы, необходимые для смягчения или уменьшения размера происшествия.

3. Восстановление деятельности — определяет последовательность действий, которые необходимо осуществить для того, чтобы восстановить сервис на заданном уровне.

Примерная структура плана обеспечения непрерывности бизнеса:

1. Введение
1.1. Исходная информация
1.2. Границы действия плана
1.3. Предпосылки создания плана
2. Концепция
2.1.Описание системы обеспечения непрерывности
2.2.Описание этапов восстановления непрерывности
2.3.Роли и их обязанности
3. Активация плана
3.1.Критерии и порядок активации
3.2.Порядок уведомления заинтересованных лиц
3.3.Порядок оценки происшествия
4. Контроль
5. Восстановление
5.1.Последовательность восстановления непрерывности

Специалистами NIST было разработано руководство , которое достаточно подробно описывает необходимые) планы обеспечения непрерывности бизнеса. Далее приведена таблица 4.5.1, где описан каждый из планов (указанных в руководстве NIST), а также даны ссылки на стандарты / НПА, которые предписывают разработку таких планов.

Таблица 4.5.1 Планы обеспечения непрерывности бизнеса

Наименование плана	Описание плана	Стандарт/ НПА
Business Continuity Plan (BCP)	Набор задокументированных процедур, которые	ISO 22301 «Социальная безопасность. Системы

План обеспечения непрерывности бизнеса	разработаны, обобщены и актуализированы с целью их использования в случае возникновения инцидента, и направлены на обеспечение возможности продолжения выполнения компанией критических важных видов деятельности на установленном приемлемом уровне.	менеджмента непрерывности бизнеса»: 8.4.4 Планы непрерывности бизнеса (Business continuity plans)
Continuity of Operations Plan (COOP) План непрерывность операций	Фокусируется на восстановлении критически важных функций компании на альтернативной площадке и на их выполнении в течение 30 дней.	-
Crisis Communication Plan План антикризисных коммуникаций	В данном плане задокументированы процедуры и правила внешних и внутренних коммуникаций в случае чрезвычайных ситуаций.	Федеральный закон от 21.12.1994 № 68 «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»: Статья 14. Обязанности организаций в области защиты населения и территорий от чрезвычайных ситуаций («Организации обязаны предоставлять в установленном порядке информацию в области защиты населения и территорий от чрезвычайных ситуаций, а также оповещать работников организаций об угрозе возникновения или о возникновении

		чрезвычайных ситуаций»).
Critical Infrastructure Protection Plan (CIP) План защиты критических инфраструктур	План направлен на защиту ключевых ресурсов и компонентов национальной инфраструктуры.	Указ Президента Российской Федерации от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».
Cyber Incident Response Plan План реагирования на кибер-инциденты	План, описывающий процедуры реакции на инциденты, связанные с атаками хакеров, вторжения в информационную систему и другие проблемы безопасности.	ГОСТ Р ИСО/МЭК ТО 18044—2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»; NIST 800-61 «Computer Security. Incident Handling Guide».
Disaster Recovery Plan (DRP) План восстановления после сбоя	План восстановления инфраструктуры компании после возникновения аварии.	ISO 22301 «Социальная безопасность. Системы менеджмента непрерывности бизнеса»: 8.4.5 Восстановление (Recovery).
Information System Contingency Plan (ISCP) План на случай непредвиденных ситуаций в информационных системах	План восстановления системы, сетей и основных приложений после аварии. Данный план необходимо разработать для каждой критической системы и/или приложения.	-

Occupant Emergency Plan (OEP) План действия персонала в случае чрезвычайной ситуации	В данном плане определяется порядок обеспечения безопасности персонала и процедуры эвакуации в случае чрезвычайных ситуаций.	Федеральный закон от 21.12.1994 г. № 68 «О защите населения и территории от чрезвычайных ситуаций природного и техногенного характера»; Федеральный закон от 21.12.1994 № 69 «О пожарной безопасности».

Вышеперечисленные документы составляются исходя из потребностей компании, но на практике чаще всего применяются следующие виды планов:

- План реагирования на инциденты – данный вид плана может включать в себя план реагирования на кибер-инциденты, план на случай непредвиденных ситуаций в информационных системах. Данный план поможет уменьшить масштабы катастрофы и смягчить ее последствия, что даст возможность сэкономить время и дополнительное преимущество при активации остальных типов планов;
- План действия персонала в чрезвычайных ситуациях – в соответствии с требованиями Федерального закона от 21.12.1994 г. №68 68 «О защите населения и территории от чрезвычайных ситуаций природного и техногенного характера» и Федерального закона от 21.12.1994 г. №69 «О пожарной безопасности» этот план является обязательным для всех компаний;
- План восстановления после сбоя – сфокусирован на восстановлении критически важных информационных систем. Данный вид плана осуществляет поддержу плана обеспечения непрерывности бизнеса и направлен на восстановление работоспособности отдельных систем и приложений;
- План обеспечения непрерывности бизнеса – сфокусирован на поддержке бизнес-процессов компании во время и после чрезвычайной ситуации; направлен на обеспечение возможности продолжения выполнения компанией критических важных для нее видов деятельности на установленном приемлемом уровне;

— План антикризисных коммуникаций – данный план поможет сохранить репутацию компании в кризисной ситуации. В нем документируется порядок взаимодействия со СМИ, правоохранительными органами, МЧС и т.д.

На этапе составления планов непрерывности бизнеса некоторые компании сосредоточиваются на технических решениях и не придают значения организационным мерам. В связи с этим необходимо указать на необходимость применения организационных мер наравне с техническими. Для этого

проводятся обучающие семинары, тестирование планов, выпускаются учебные материалы.

6. Тестирование и пересмотр планов

Тестирование осуществляется для проверки работоспособности планов при возникновении определенного набора обстоятельств, влияющих на деятельность компании. План тестирования выбирается с учетом типа компании и ее целей.

Тесты — инструменты оценки, которые используют количественные метрики для проверки работоспособности ИТ-системы или ее компонента.

К целям тестирования можно отнести:

- получение подтверждений работоспособности планов;
- проверка достаточности методического и технического обеспечения;
- получение необходимых навыков и знаний.

После того как была определена цель тестирования, разрабатывается сценарий, определяется метод тестирования и согласовывается с руководством. Чаще всего применяются следующие методы :

- Настольная проверка (Tabletop);
- Имитация (Imitation);
- Полное тестирование (Full business continuity testing).

После проведения тестирования составляются отчеты, в которых указываются сценарии и результаты тестирования, а также предложения по улучшению планов непрерывности деятельности.

Компании должны выбирать способ тестирования исходя из своих целей и финансовых возможностей.

Полное тестирование является самым эффективным так как оно позволяет выявить множество недостатков, но из-за высоких рисков почти не используется на практике. Если компания решила использовать данный вид тестирования, необходимо заручиться поддержкой партнеров или воспользоваться услугами подрядчиков, чтобы минимизировать риски и предупредить значительные простои.

7. Обслуживание и обновление планов

Как уже отмечалось выше, управление непрерывностью бизнеса компании является циклическим процессом. А это значит, что нельзя ограничиваться одним только формированием планов, необходимо сопровождать, обновлять и совершенствовать их ежегодно, а иногда и чаще, например, в следующих случаях:

1. Изменение ИТ-инфраструктуры;
2. Изменение организационной структуры компании;
3. Изменения в законодательстве;
4. Обнаружение недостатков в планах при их тестировании.

Чтобы сохранить актуальность планов, необходимо выполнять следующие действия:

- проводить внутренние аудиты, включающие проверку восстановления после аварий, документации по обеспечению непрерывности и соответствующих процедур;
- проводить регулярные практические тренинги по выполнению плана;
- интегрировать вопросы непрерывности бизнеса в процесс управления изменениями компании.

Управление непрерывностью бизнеса обеспечивает объединение всех применяемых на предприятии мер в целостный, адекватный реальным угрозам и управляемый комплекс, позволяющий компании непрерывно предоставлять услуги, избежать влияния чрезвычайных ситуаций на деятельность и минимизировать возможный ущерб.

Оглавление

1. Введение 1
1.1. Ретроспектива проблемы опеспечения безопасности в инфокоммуникациях. 1
1.2. Облачные вычисления 2
1.3. Определение безопасности 7
2.Классификация угроз, атак и защищяемой информации. 13
2.1. Источники и типы угроз 13
2.2. Этапы атаки 21
2.3. Взлом паролей 23
2.4. DDOS атаки 27
2.5. Ботнет 32
2.6. Классификация защищаемой информации 35
3. Риск. Политика информационной безопасности. 38
3.1. Понятие риска 38
3.2. Оценка риска 40
3.3 Обработка рисков 55
3.4. Политика информационной безопасности 68
3.5. Осведомленность сотрудников по информационной безопасности 70
4. Технологии защиты 73
4.1. Аутентификация. Управление доступом. 73
4.2. Безопасность клиетских устройств.Антивирусы. 84
4.3. Сетевая защита 89
4.4. Криптографические методы защиты информации 101
4.5.Управления непрерывностью бизнеса 110