Информационная безопасность для ИТ-шника

HTTP://WWW.FACEBOOK.COM/ANDREY.A.KONDRATENKO
(ANDREY.KONDRATENKO@GMAIL.COM)

Глава 1

Информационная безопасность для ИТ-шника

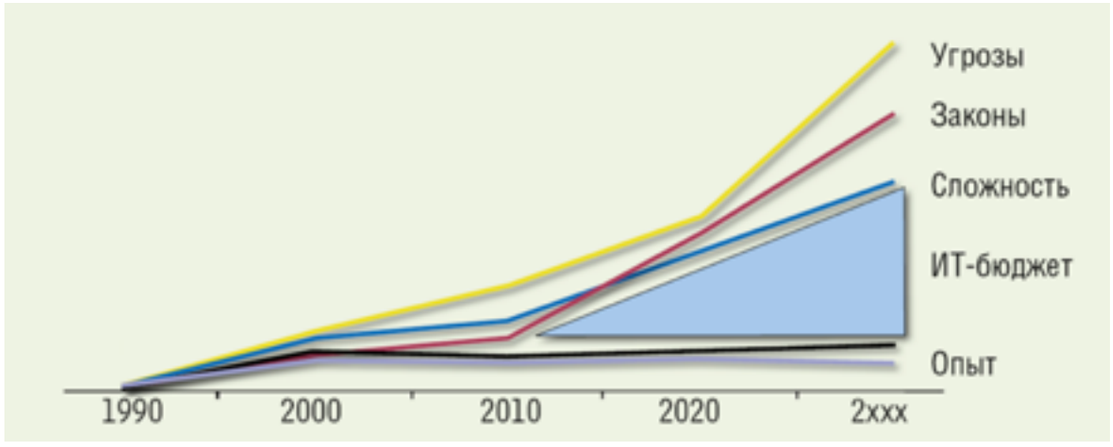
Многие рассматривают информационную безопасность по остаточному принципу, зачастую совсем про нее забывая.

Вот и мы посмотрим, как лучше поступить.

Раздел 1

Что такое информационная безопасность?

Прогресс в области информационных технологий (ИТ) , несомненно , приводит к повышению конкурентоспособности организаций их применяющих. Вместе с тем, наряду с получаемыми преимуществами от развития ИТ, организации подвергаются новым рискам, связанным с **безопасностью** хранимой, обрабатываемой и передаваемой информации, критичной с точки зрения возможных последствий для бизнеса.



Отставание средств защиты от актуальных угроз (по данным IDC) (Статья «Журнал сетевых решений/LAN» , № 01, 2012: http://www.osp.ru/lan/2012/01/13012473/).

По прогнозу аналитиков Gartner, мировые расходы на информационную безопасность (ИБ) в течение 5 лет вырастут на 58% по сравнению с 2010 годом и по итогам 2015 года превысят $49,1 млрд. Наиболее высокие темпы роста продемонстрирует сегмент услуг аутсорсинга управления ИБ - он вырастет более, чем в 2 раза с 2010 по 2015 год: с $6,82 млрд до $14,89 млрд. Основная причина такого роста – это ущерб, который наносят компаниям по всему миру утечки и утери информации.

Так что же такое **информационная безопасность**, как ей нужно управлять и исходя из каких критериев планировать бюджет на эту задачу?

Исторически информационная безопасность возникла с момента возникновения средств информационных коммуникаций между людьми, а также с наличием у людей интересов, которым может быть нанесен ущерб путем воздействия на информацию и на средства, которыми эта информация доставлялась. То есть фактически ИБ появилась раньше информационных технологий. Но вот уже более века, с момента появления радиосвязи, развитие информационной безопасности непрерывно и неотделимо связано с развитием информационных технологий.

Что защищать?

С точки зрения владельцев бизнеса, объектом защиты всегда является информация, потеря, огласка или подмена которой, может нанести ущерб для бизнеса и

владельца в стоимостном выражении. Информация может существовать в различных формах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных средств связи , демонстрироваться на пленке или быть выражена устно.

В терминах информационной безопасности, под **объектом защиты** понимается информация - сведения (сообщения, данные) независимо от формы их представления[4].

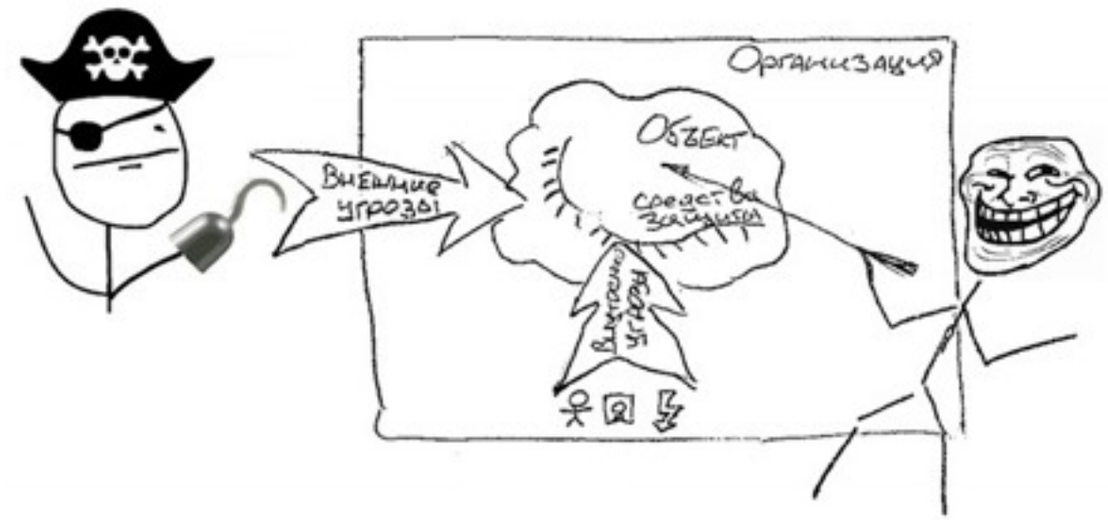
Безотносительно формы выражения информации, средств ее распространения или хранения, она должна быть всегда адекватно защищена [1]. С точки зрения информационных технологий , защищенность информации является результатом реализации комплекса политик и процедур, разработанных для идентификации, управления и защиты информации совместно с любым оборудованием и программным обеспечением, используемым для ее хранения, передачи и обработки [3]. Таким образом, объектом внимания информационной безопасности в сфере ИТ будут являться средства, участвующие в процессе обработки (хранения, передачи) информации: носители (жесткие диски, флешки, ленты и т.д.), программные средства (ОС, СУБД, прикладное ПО и т.д.), каналы связи (локальные вычислительные сети, каналы передачи данных и т.д.), оборудование (ПК, серверы и т.д.).

Информационная безопасность (ИБ) – это деятельность, направленная на защиту информации от широкого диапазона угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации ущерба, получения максимальной отдачи от инвестиций, а также реализации потенциальных возможностей бизнеса [1].

Обеспечение информационной безопасности – это непрерывный процесс достижения установленного состояния **конфиденциальности** (избежание несанкционированного разглашения) , **целостности** (избежание несанкционированной модификации) и **доступности** (обеспечение беспрепятственного доступа) информации.

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационной безопасностью , которые могут быть представлены политиками , методами , процедурами , организационными структурами и функциями программного обеспечения.

Угрозы информационной безопасности



От чего защищать информацию?

Информацию необходимо защищать от угроз, где **угроза безопасности информации** – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации[2]. Угрозы могут быть разных типов : несанкционированное воздействие на информацию (сбор, уничтожение, повреждение), воздействие на программы (вирусы), воздействие на носители (кража, повреждение), воздействие на компьютеры (повреждение), разглашение информации преднамеренное или непреднамеренное («от не знания») и т.д. Источником угрозы безопасности информации может выступать субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации [2]. Угроза может нарушить конфиденциальность (перехват или хищение информации), целостность (искажение информации), доступность информации (блокирование доступа). Источник угроз может быть внешний (конкуренция, стихийное бедствие, не преследующие цели DDOS атаки) и внутренний (недостаточная компетенция, халатность, злой умысел).

Условием реализации **угрозы** безопасности к информационной системе информации может быть недостаток или слабое место в информационной системе, называемое **уязвимостью** [2].

Уязвимость – это свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации[2].

Угрозы приводят к рискам информационной безопасности.

Риском информационной безопасности называется возможность того, что **угроза** сможет воспользоваться **уязвимостью** актива или группы активов и тем самым нанесет **ущерб** организации[5].

Под **ущербом** (в гражданском праве) понимаются невыгодные для собственника имущественные

последствия, возникшие в результате причинения ему вреда. **Ущерб** выражается в уменьшении имущества либо в недополучении дохода, который был бы получен при отсутствии нарушения (упущенная выгода). **Ущерб** может быть материальным и настать для собственника или контрагента , моральным или физическим , порочащим деловую репутацию , экологическим , социальным и т.д.

Причиненный **ущерб** может быть квалифицирован как состав преступления, предусмотренный уголовным правом , или сопоставляться с рисками утраты , предусмотренными гражданским или административным правом.

Не все идентифицированные **угрозы** одинаково осуществимы и могут привести к одинаковому **ущербу**. Для принятия оптимизированных решений по уменьшению **угроз** информационной безопасности применяется подход , при котором решения принимаются по результатам **оценки рисков** информационной безопасности.

Оценка рисков — процесс, предназначенный для идентификации источников рисков и определения его уровня значимости. Оценку рисков разбивают на **анализ рисков** и **оценивание рисков**.

1. Анализ рисков

Анализа рисков, подразделяется на два этапа:

- **Определение стоимости защищаемых ресурсов**. Проводится инвентаризация и категоризация защищаемых ресурсов , выяснение нормативных , технических, договорных требований к ресурсам в сфере ИБ. Затем с учетом этих требований определяется стоимость ресурсов . В стоимость входят все потенциальные потери , связанные с возможной компрометацией защищаемых ресурсов.

- **Моделирование угроз информационной безопасности**. Следующим этапом анализа рисков является составление перечня значимых угроз и уязвимостей для каждого ресурса, а затем вычисление вероятности их реализации (моделирование угроз информационной безопасности). Для решения этой задачи разрабатывается модель угроз ИБ к конкретному защищаемому ресурсу.

Модель угроз информационной безопасности – это описание существующих угроз ИБ, их актуальности, возможности реализации и последствий.

Цель разработки модели угроз – определение актуальных для конкретной информационной системы угроз безопасности, источников угроз и уязвимостей. Результаты моделирования используются для классификации информационных систем, а также в качестве исходных данных для построения (проектирования) обоснованной и эффективной системы защиты информационной системы.

Отрицательное воздействие угроз информационной безопасности уменьшается различными методами, направленными, с одной стороны, на уменьшение воздействия со стороны источников угроз, а с другой - на устранение или существенное ослабление факторов их реализации – уязвимостей. Кроме того, эти методы должны быть направлены на устранение последствий реализации угроз.

Существует масса методик построения моделей угроз, но выбирать все же стоит, исходя из категории защищаемых данных, специфики своей отрасли, а также требований регуляторов , если такие имеются у организации (например: руководящие документы ФСТЭК России и ФСБ России, ГОСТ, ISO/IEC, банковские стандарты и т.д.).

В случае, когда в организации нет ресурсов на построение модели угроз, при создании системы защиты рекомендуется придерживаться нескольких общих рекомендаций по достижению установленной защищенности информации:

- **конфиденциальности** – путем защиты от несанкционированного доступа и шифрования информации в виде документов и каналов связи;

- **целостности** – путем использования электронной подписи для документов и каналов связи;

- **доступности** – путем резервирования компонентов информационной системы и каналов связи, восстановлением в случае сбоев.

2. Оценивание риска

Оценивание риска проводится путем его вычисления и сопоставления с заданной шкалой. Вычисление риска состоит в умножении вероятности компрометации ресурса на значение величины ущерба, связанного с его компрометацией. Сопоставление риска выполняется с целью упрощения процесса использования на практике точечных значений риска [5].

Допускается использование как количественных, так и качественных методов оценки рисков. Но основной информацией для таких методов все равно будет экспертная оценка, позволяющая оценить стоимость идентифицированного ресурса и уровень вероятности угрозы. Совокупность этих показателей и будет составлять уровень риска, по которому проводится ранжирование.

После того, как риск оценен, должно быть принято решение относительно его обработки — точнее, выбора и реализации мер и средств по минимизации риска. Помимо оцененного уровня риска, при принятии решения могут быть учтены затраты на внедрение и сопровождение механизмов безопасности, политика руководства, простота реализации, мнение экспертов и др. В зависимости от итогов оценки, может быть

определен один из четырех вариантов обработки реакции на риска:

- **уменьшение риска** - риск считается неприемлемым, и для его уменьшения выбираются и реализуются соответствующие меры и средства безопасности;

- **передача риска** - риск считается неприемлемым и на определённых условиях (например, в рамках страхования, поставки или аутсорсинга) предается сторонней организации;

- **принятие риска** - риск в данном случае считается осознанно допустимым - организация должна смириться с возможными последствиями (обычно это означает , что стоимость контрмер значительно превосходит финансовые потери в случае реализации угрозы, либо организация не может найти подходящие меры и средства безопасности);

- **отказ от риска** – отказ от бизнес-процессов организации, являющихся причиной риска (например, отказ от обработки информации о состоянии здоровья работника в сети).

В результате обработки риска остается так называемый остаточный риск, относительно которого принимается решение о завершении этапа отработки риска. Управление рисками осуществляется состоит в путем комбинированияи предупредительных и корректирующих механизмов контроля , тактики избегания, принятия или передачи риска другой организации (аутсорсинг информационной безопасности). Помимо оцененного уровня риска, при принятии решения могут быть учтены затраты на внедрение и сопровождение механизмов безопасности, политика руководства, простота реализации, мнение экспертов и др. В результате обработки риска остается так называемый остаточный риск, относительно которого принимается решение о завершении этапа отработки риска.

В случае выбора тактики уменьшения риска, отрицательное воздействие рисков уменьшается различными методами, направленными:

- на уменьшение воздействия со стороны источников угроз;

- на устранение или существенное ослабление факторов их реализации – уязвимостей;

- на устранение последствий реализации угроз.

При планировании мер по обработке риска, желательно провести ранжирование таких мер на первоочередные, среднесрочные и долгосрочные меры:

- **первоочередные мероприятия** должны позволять снизить часть рисков без затрат, за короткий промежуток времени (например, не более одного месяца – выпуск локального нормативного акта, содержащего организационные мероприятия);

- **среднесрочные мероприятия** должны позволить снизить следующую часть рисков за непродолжительный промежуток времени в рамках запланированного бюджета (например, в течение финансового года путем перераспределения финансовых средств с других статей расходов на закупку ПО или оборудования);

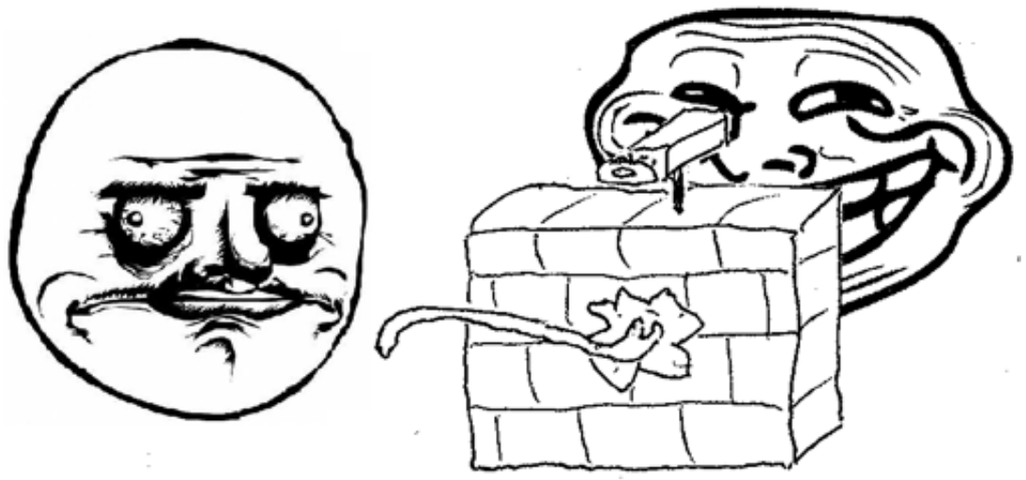
- **долгосрочные мероприятия** должны снижать риск до приемлемого в перспективе (например, путем планирования в инвестиционную программу будущих лет выполнения проекта по защите).

Решения о выборе мер противодействия угрозам информационной безопасности должны приниматься совместно с владельцами деловых процессов, нарушение или неверное функционирование которых может привести к ущербу.

В случае, если присутствуют существенные риски, для которых необходимо непредвиденное вливание денежных средств (например, уход с рынка антивирусной компании или предписание регулирующих органов), решение о финансировании или принятии риска должно приниматься высшим руководством компании (CEO, Совет Директоров и т.д.).

При внедрении новых информационных систем рекомендуется учитывать требования информационной безопасности на этапе создания, потому что это обойдется дешевле и будет эффективнее по затраченным ресурсам и срокам по сравнению с учетом таких требований в системе уже внедренной в эксплуатацию.

Методы и средства защиты информации



Среди методов защиты информации можно выделить правовые (заключение соглашений , категорирование и присваивание грифа информации), экономические (страхование рисков), организационные (изменение оргструктуры , внедрение политик и инструкций и пр.), технические (использование средств защиты информации и пр.) и т.д.

К организационным методам защиты можно отнести : выделение организационной структуры , отвечающей за обеспечение информационной безопасности организации; назначение персональной ответственности работников за сохранность информации; организация регламентированного доступа пользователей к работе с компьютерами; установление запрета на использование открытых каналов связи для передачи конфиденциальной информации и т.д. Без надлежащего обеспечения организационных мер , невозможно эффективно применять технические методы защиты. При отсутствии технических методов защиты, организационные методы на первом этапе позволяют повысить ИБ (например: запрет выхода в интернет и использования флеш - носителей) , но существенно затрудняют обработку информации , поэтому технические методы защиты должны быть неотрывно связаны с организационными.

Технические методы защиты информации можно разделить на методы защиты информации от несанкционированного доступа (обеспечение целостности, доступности, конфиденциальности) и от утечки по техническим каналам (защита от побочного электромагнитного излучения и наводок, защита речевой и видовой информации и пр.).

Так, в общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от несанкционированного доступа традиционно реализуется следующими подсистемами [7]

- подсистема управления доступом (ПУД);
- подсистема регистрации и учета (ПРУ);
- подсистема обеспечения целостности (ПОЦ);

- подсистема криптографической защиты (ПКЗ).

Требования к подсистемам могут быть разработаны в зависимости от уровня важности информации, обрабатываемой в системе, уровня полномочий субъектов доступа к информации, режима обработки данных (коллективный или индивидуальный).

Подсистема управления доступом (ПУД) – должна осуществлять идентификацию , проверку подлинности и контроль доступа субъектов в систему, устройствам, программам, файлам и т.д. в зависимости от класса защищаемой автоматизированной системы. Такая проверка осуществляется механизмами аутентификации с использованием паролей, сертификатов, биометрии, карт доступа и т.д. Чем сложнее и важнее информационная система, тем более могут ужесточаться требования по управлению доступом.

Подсистема регистрации и учета (ПРУ) – должна осуществлять контроль входа/выхода субъектов в/из защищаемой автоматизированной системы . Это подсистема журналирования, которая, в зависимости от сложности поставленных задач, может вести журналы от входа и выхода пользователей в систему - в самых простых случаях, до подробного журналирования всех действий всех субъектов информационного взаимодействия с информацией (добавление , удаление , изменение просмотр, печать и т.д.).

Подсистема обеспечения целостности (ПОЦ) – должна обеспечивать целостность программных средств защиты информации , самой обрабатываемой информации, а также неизменность программной среды.

Целостность обычно проверяется при загрузке операционной или информационной системы путем сравнения контрольных сумм (CRC) программ и информации в самых простых случаях. Целостность обеспечивается, в том числе путем размещения средств обработки информации не в общедоступном месте (серверная, комната, запираемая на ключ).

К более серьезным системам разрабатываются требования по оперативному контролю и воздействию на безопасность автоматизированных систем , периодическому тестированию функций защиты с помощью специальных программных средств, наличию автоматических средства восстановления при сбоях. Это особенно актуально для систем удаленного обслуживания - таких как терминалы банковского обслуживания, для которых сложно обеспечить физическую защиту от вмешательства и оперативный выезд специалиста.

Перечисленные подсистемы ПУД, ПРУ, ПОЦ, в зависимости от требований по информационной безопасности к информационным системам, могут быть реализованы:

- средствами операционной системы, специально настроенной в соответствии с требованиями /

рекомендациями руководящих документов по безопасной настройке и контролю ОС;

- специализированными средствами защиты информации;

- средствами информационной системы, путем приведения ее в соответствие требованиям руководящих документов.

Подсистема криптографической защиты (ПКЗ) – должна обеспечивать шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа.

ПКЗ, помимо повышения конфиденциальности информации перечисленными выше способами , позволяет повысить и целостность информации - путем использования такого свойства средств криптографической защиты информации , как электронная подпись . Использование электронной подписи позволяет защитить информацию в электронном виде от подделок.

К не перечисленным выше способам и методам защиты информации также относятся:

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок , использование средств антивирусной защиты;

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности;

- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

- резервирование технических средств , дублирование массивов и носителей информации;

- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

- использование защищенных , выделенных , дублируемых каналов связи;

- организация физической защиты помещений и собственно технических средств;

- анализ защищенности информационных систем , предполагающий применение специализированных программных средств (сканеров безопасности)и т.д.

Перечислим наиболее известные системы , используемые для обеспечения защиты информации.

Подсистема антивирусной защиты – комплекс программно - аппаратных средств для обнаружения компьютерных вирусов , а также нежелательных (считающихся вредоносными) программ вообще , восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Хорошим примером для организации, выходящей в сеть Интернет , может служить создание эшелонированной антивирусной защиты , где оборонительными эшелонами являются:

- почтовые и интернет-шлюзы, проверяющие входящий трафик из сети Интернет (в том числе, и на наличие спама);
- антивирус на почтовом сервере, проверяющий почтовые сообщения;
- антивирус на файловых серверах, серверах приложений и баз данных;
- антивирус на рабочих станциях.

Межсетевой экран (брандмауэр, файервол) - обеспечивает защиту автоматизированной системы посредством фильтрации трафика к информационному ресурсу или между сетями [7].

Для эффективной работы межсетевой экран должен быть настроен по соответствующему классу защищенности, необходимому организации, и на межсетевом экране должен быть настроен список контроля доступа , соответствующий политике безопасности организации . Должен проводиться периодический контроль изменений межсетевого экрана.

Использование межсетевых экранов , их своевременная настройка и контроль позволяют повысить защищенность информационных систем от несанкционированного доступа к информации со стороны вычислительных сетей.

Межсетевые экраны « нового поколения » характеризуются переходом от пакетной фильтрации на уровне IP адресов и портов к фильтрации трафика на уровне приложений (7-м уровне сетевой модели OSI), где применение политик безопасности (разрешить / запретить) происходит отдельно для каждого процесса или приложения. Такие межсетевые экраны позволяют проводить также более гибкую интеграцию со шлюзовыми системами антивирусной защиты и системами обнаружения и предотвращения вторжений.

При покупке межсетевого экрана стоит обратить внимание на то, требуется ли в Вашей информационной системе межсетевой экран, сертифицированный в органах ФСТЭК России, и по какому классу, потому что не все они смогут пройти такую сертификацию. Можно купить сертифицированный межсетевого экрана или провести сертификацию с привлечением соответствующего лицензиата. Главное - не забывать, что, во-первых, сертифицированный межсетевой экран еще должен быть настроен на соответствие своему классу, а во-вторых, сертификат не вечен и через три года его придется продлить.

Прокси-серверы – обычно применяются в сети для обеспечения доступа с компьютеров локальной сети в Интернет. Такой подход позволяет с одной стороны защищать клиентский компьютер от некоторых сетевых атак, а с другой стороны - помогает наладить в организации учет трафика каждого конкретного сотрудника. Доступ в сеть Интернет работников организации должен быть организован таким образом, чтобы все выходили в сеть через прокси-сервер, причем входящий трафик должен проверяться антивирусом интернет-шлюза.

Система обнаружения вторжений (СОВ) – предназначена для предотвращения и / или детектирования несанкционированного доступа к информационным ресурсам . Компоненты системы обнаружения вторжений СОВ более известны как IPS (Intrusion prevention system – система предотвращения вторжений) и IDS (Intrusion detection system – система обнаружения вторжений). Технически один и тот же компонент может выполнять обе роли – предотвращения и обнаружения, тогда в первом случае он ставится в разрез принимаемого трафика, а во втором случае работает с зеркальной копией трафика.

Однако стоит обратить внимание, что при установке компонентов в режиме IPS может резко снизиться доступность распределенной информационной системы. Это происходит в том случае, если изменения в системе происходят часто и не контролируются теми, кто настраивает фильтры сигнатур, а также в случае выхода новых сигнатур обнаружения вторжений.

Подсистема анализа защищенности (сканирования уязвимостей) – предназначена для контроля настроек защиты операционных систем на рабочих станциях и серверах и позволяет оценить возможность проведения нарушителями атак на сетевое оборудование, а также контролирует безопасность программного обеспечения. С помощью таких средств производится сканирование сети с целью исследования ее топологии, осуществления поиска незащищенных или несанкционированных сетевых подключений, проверки настроек межсетевых экранов и т.п. Данный анализ производится на основании детальных описаний уязвимостей настроек средств защиты (например, коммутаторов, маршрутизаторов, межсетевых экранов) или уязвимостей операционных систем или прикладного программного обеспечения. Результатом работы средств

анализа защищенности является отчет, в котором обобщаются сведения об обнаруженных уязвимостях.

Средства сканирования уязвимостей могут функционировать на сетевом уровне , уровне операционной системы и уровне приложения. Применяя сканирующее ПО, можно составить карту доступных узлов информационной системы, выявить используемые на каждом из них сервисы и протоколы, определить их основные настройки и сделать предположения относительно вероятности реализации несанкционированного доступа . По результатам сканирования системы вырабатываются рекомендации и меры, позволяющие устранить выявленные недостатки.

Подсистема анализа защищенности должна давать администраторам сети представления об уязвимых местах и устаревшем программном обеспечении. Служба безопасности должна контролировать процесс устранения найденных уязвимостей и ставить CIO в известность об эффективности работы его сотрудников.

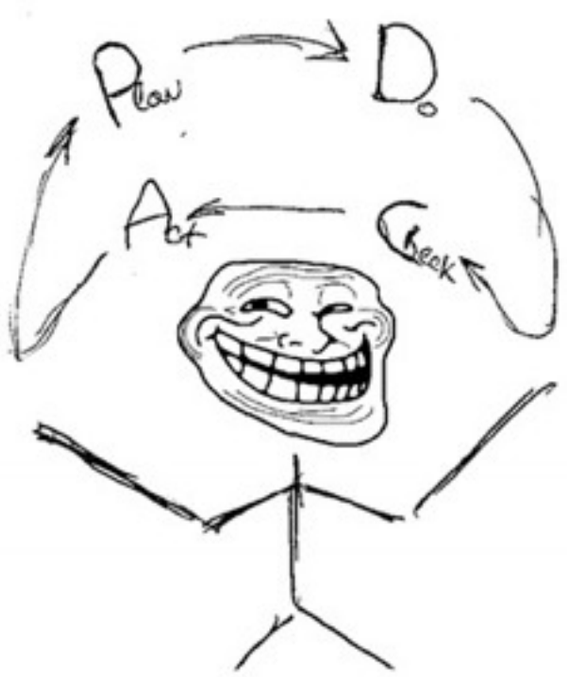
Предотвращения утечек информации (DLP) — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

Системы DLP (Data Leak Prevention) - строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы . При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется , либо администратору безопасности сообщается о такой попытке.

С применением данных, полученных D L P необходимо быть достаточно осторожным, потому что деятельность по сбору информации о преступных посягательствах попадает под Федеральный закон «Об оперативно-розыскной деятельности» и для проведения оперативно-розыскных мероприятий должны иметься серьезные основания и необходимая компетенция. Поэтому с работника необходимо взять письменное согласие на то, что информация, обрабатываемая на его компьютере, будет перлюстрироваться.

Комбинация перечисленных выше систем позволяет обеспечить достаточно хорошую защиту информации при условии наличии в организации специалистов высокого уровня, достаточного бюджета и времени. В любой организации можно существенно повысить информационную безопасность , изначально сконцентрировавшись на трех подсистемах: подсистеме управления доступом, подсистеме антивирусной защиты и подсистеме межсетевого экранирования.

Организация информационной безопасности



Информационная безопасность идет бок о бок с информационными технологиями и даже международный стандарт для управления и обслуживания ИТ сервисов ISO 20000 рассматривает ИТ-безопасность как один из процессов предоставления услуг.

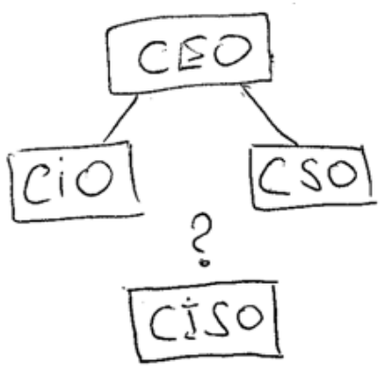
Но в то же время, не стоит смешивать понятия информационной безопасности и ИТ-безопасности. Вопросы информационной безопасности включают в себя ИТ-безопасность, но не ограничиваются ей, захватывая области, не относящиеся к ИТ (например: защита бумажных документов , защита от побочных электромагнитных излучений и наводок, аттестация объектов информатизации, и помещений и пр.).

Как правило, в каждой компании существует CSO (Chief Security Officer) — главный руководитель в области безопасности организации, отвечающий за вопросы информационной безопасности , физической безопасности, экономической безопасности, гражданской обороны и чрезвычайных ситуаций и т.д. При этом, согласно международной практике, для направления информационной безопасности выделяется отдельный руководитель - CISO (Chief Information Security Officer). Кому CISO должен подчиняться - CIO или CSO на этот вопрос существуют различные точки зрения. CIO стремится подчинить CISO себе, чтобы информационная безопасность не мешала развитию ИТ. В свою очередь CSO стремиться подчинить CISO себе, чтобы информационная безопасность контролировала развитие ИТ и обеспечивало ее безопасность.

К сожалению, как показывает практика, при интенсивном развитии информационных технологий в организации приоритетным становится обеспечение доступности информации, а вопросы обеспечения конфиденциальности и целостности отходят на второй

план или забываются до поры до времени забываются. При таком подходе часто можно встретить « автоматическое » подчинение всего направления информационной безопасности CIO. Однако, это нередко приводит к непоправимым нарушениям целостности информации, утечкам данных и невосполнимым крахам систем и информации в них, ведь никто не может контролировать сам себя должным образом. Поэтому, в международной практике преобладает подчинение CISO именно CSO, так как, помимо очевидного выравнивания баланса обеспечения доступности , целостности и конфиденциальности, это дает еще и эффективные механизмы контроля для CEO и CIO за деятельностью всей сферы ИТ. В целом, этот вопрос должен решаться в зависимости от динамики развития компании. Для достаточно стабильного бизнеса логичным выглядит подчинение руководителя по информационной безопасности (CISO) блоку общей безопасности (CSO). Но если компания активно развивается и скорость развития играет очень большую роль, то, возможно, оптимальнее будет подчинение CISO CIO.

При любом варианте подчинения при исполнении повседневных функциональных обязанностей CISO тесно взаимодействует со службами ИТ, подчиняющимися CIO. CISO, фактически, задает требования к ИБ и контролирует их выполнение (рассмотрение технических заданий, участие в приемке ИС, проведение проверок и т.д.), а службы ИТ являются руками CISO по технической реализации этих правил (там, где вопросы ИБ касаются сферы ИТ). При взаимодействии с остальными работниками компании CISO должен быть нацелен на повышение осведомленности работников по вопросам информационной безопасности (путем выпуска локальных нормативных актов, политик осведомленности , проведения инструктажей и т.д.).



CISO должен иметь хорошее техническое образование и опыт, позволяющее не только общаться со службами ИТ на одном языке, но и предлагать решения по выходу из ситуаций, которые могли бы нарушить режим информационной безопасности. Кроме того, CISO должен хорошо ориентироваться в вопросах законодательства в области ИБ, т.к. важной его задачей в крупной компании является также взаимодействие по вопросам обеспечения информационной безопасности с государственными регулирующими органами – такими, как ФСБ России, ФСТЭК России, Роскомнадзор и т.д.

При организации работ по обеспечению информационной безопасности должны быть определены цели и задачи информационной безопасности, изложены наиболее существенные для организации принципы , правила и требования информационной безопасности. Обычно для этого выпускается документ верхнего уровня по информационной безопасности, называемый Концепция

или Политика информационной безопасности , отвечающий на поставленные вопросы.

Политика информационной безопасности должна быть утверждена, издана и надлежащим образом доведена до сведения всех сотрудников организации. Она должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью [1].

При формулировании требований информационной безопасности необходимо расставить приоритеты обеспечения информационной безопасности (например, для банков это может быть соблюдение отраслевых стандартов, для государственных компаний – соблюдение федерального законодательства, для частных компаний - соответствие внутренним корпоративным нормам и правилам и т.д.).

Если для вашей организации не предусмотрено никаких стандартов , начните формировать свои внутренние корпоративные нормы и правила информационной безопасности исходя из национальных стандартов. , даже если не все требования покажутся вам целесообразными , вы всегда сможете отыскать требования, которые подошли бы именно для вашей организации и они не будут взаимоисключающими с требованиями российского законодательства. Либо же, стоит обратить внимание на то, какие проверяющие органы могут проводить проверку состояния вашей информационной безопасности, у проверяющих органов тоже есть перечень рекомендаций и методик , построенных на стандартах и руководящих документах.

Для планирования, реализации и поддержки решений информационной безопасности должны быть назначены работники , обеспечивающие информационную безопасность , установлена ответственность за нарушение информационной безопасности.

Для того , чтобы меры по соблюдению информационной безопасности были наиболее эффективными, их актуальность должна периодически проверяться и пересматриваться. Эффективность мер по информационной безопасности можно повысить, создав систему менеджмента информационной безопасности. Для удобства управления жизненным циклом информационной безопасности удобно использовать процессный подход к разработке , внедрению , обеспечению функционирования, мониторингу, анализу, поддержке и улучшению системы управления [6]. Процессная модель «**Планирование** (Plan) – **Реализация** (Do) – **Проверка** (Check) – **Действие** (Act)» PDCA может быть применена при структурировании всех процессов управления ИБ.

- **Планирование** (создание системы менеджмента информационной безопасности) – определение политики информационной безопасности, целей, процессов и процедур, относящихся к управлению рисками и совершенствованию ИБ.

- **Реализация** (внедрение и эксплуатация системы менеджмента информационной безопасности) – внедрение и эксплуатация политики ИБ, механизмов контроля, процессов и процедур.

- **Проверка** (мониторинг и анализ системы менеджмента информационной безопасности) – оценка и измерение характеристик исполнения процесса в соответствии с политикой ИБ, целями и практическим опытом, и предоставление руководству отчетов для анализа.

- **Действие** (сопровождение и совершенствование системы менеджмента информационной безопасности) – принятие корректирующих и превентивных мер , основанных на результатах внутреннего и внешнего аудитов ИБ, проверок со стороны руководства и результатах расследования инцидентов.

Внедренная система менеджмента информационной безопасности периодически должны выполнятся мониторинг и анализ для обнаружения ошибок, инцидентов информационной безопасности, оценки качества выполнения предпринимаемых мер безопасности, пересмотра рисков и планирования мероприятий обеспечению ИБ.

Для эффективного управления рисками в организации рекомендуется проводить периодический (не реже раза в год) контроль и оптимизацию рисков. Для контроля рисков рекомендуются проводить технические меры (мониторинг, анализ системных журналов и выполнения проверок), анализ со стороны руководства, независимые внутренние аудиты ИБ. Оптимизация риска содержит переоценку риска и, соответственно, пересмотр политик , руководств по управлению рисками , корректировку и обновление механизмов безопасности.

Для оценки эффективности системы менеджмента информационной безопасности должны планироваться и осуществляться внутренние и внешние аудиты. Цель внешнего аудита – убедиться в непрерывности , адекватности и эффективности применяемых в организации мер по ИБ. Внутренний аудит позволяет проверить выполнение принятых правил работниками ИТ и других сфер деятельности компании.

Чтобы система менеджмента информационной безопасности всегда отвечала текущим потребностям бизнеса в ИБ, должно осуществляться регулярное планирование ее развития и совершенствования , предприниматься соответствующие корректирующие и предупреждающие действия, обеспечиваться достижение поставленных целей.

Для систематизации работ по управлению информационной безопасности можно воспользоваться национальным стандартом РФ ГОСТ Р ИСО / МЭК 27001-2006 «Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности» [6] (является адаптацией британского стандарта BS ISO/IEC 17799-2000).

Раздел 5

Нормативное регулирование

Российское законодательство уделяет должное внимание вопросам информационной безопасности и разработало достаточное количество нормативных документов , позволяющих регулировать вопросы информационной безопасности.

К нормативно-правовым актам федерального законодательства в области информационной безопасности можно отнести международные договоры РФ, Конституцию РФ, законы федерального уровня (включая федеральные конституционные законы , кодексы) , указы Президента РФ , постановления Правительства РФ , нормативные правовые акты федеральных министерств и ведомств, нормативные правовые акты субъектов РФ , органов местного самоуправления и т. д.

Наиболее известные из них:

- Федеральный закон от 29.07.2004 № 98-ФЗ (О коммерческой тайне).
- Федеральный закон от 27.07.2006 № 149-ФЗ (Об информации, информационных технологиях и о защите информации);
- Федеральный закон от 27.07.2006 № 152-ФЗ (О персональных данных);
- Федеральный закон от 06.04.2011 № 63-ФЗ (Об электронной подписи);
- Постановление Правительства РФ от 01.11.2012 №1119 (Об обеспечении безопасности персональных данных при их обработке в ИСПДН).

Перечень не исчерпывающий, но достаточный, что бы понимать, на какие аспекты информационной безопасности организации стоит обратить внимание.

Наряду с законами и подзаконными актами, существует масса руководящих и нормативных документов (таких как: национальные стандарты (ГОСТ) в области ИБ, руководящие документы ФСТЭК России, ФСБ России, Роскомнадзор и т.д.), отраслевых стандартов по информационной безопасности(межкорпоративные

стандарты по информационной безопасности ОАО «Газпром», Банка России и т.д.), международные стандарты и пр.

Особенности обеспечения информационной безопасности в РФ вытекают из стремления контролирующих органов снять угрозы национальной безопасности от засилья иностранного аппаратного и программного обеспечения.

Для этого применятся подходы:

- недопущение на российский рынок иностранных продуктов;
- сертификация средств защиты информации.

Цель недопущения на рынок иностранных продуктов довольная ясна – это развитие отечественного производства и избегание удаленного управления программными и аппаратными средствами с использованием «закладок» по требованиям иностранных правительств.

К сожалению, развитие отечественного рынка средств защиты информации не развито на столько, чтобы вытеснить зарубежное программное и аппаратное обеспечение (как, например, это пытается делать Китай), что, в принципе касается и ИТ технологий. Поэтому приходится прибегать к сертификации ввозимых средств защиты информации, которая может занимать продолжительное время (например, ввоз межсетевого экрана с иностранной криптографией может занять 6-9 месяцев) и стоить существенных средств.

Требования по безопасности предъявляются не только к ввозимым средствам, но и к отечественным. Соответствие требованиям подтверждаются разными способами, например:

- сертификация по показателям класса защищенности средств вычислительной техники от несанкционированного доступа;
- сертификация по отсутствию незадекларированных возможностей;
- сертификация по оценочному уровню доверия (ОУД) к реализации требований по защите;
- сертификация по классу межсетевого экранирования;
- оценка соответствия требованиям к системам обнаружения вторжений и т.д.

Причем проверить соответствие реализованных функций требованиям руководящих документов и осуществить сертификацию может лишь организация, имеющая аттестат аккредитации испытательной лаборатории.

К особенностям информационной безопасности РФ можно также отнести аттестацию информационных

систем, автоматизированных рабочих мест и помещений по требованиям регулирующих органов.

К сожалению, наличие сертификата соответствия у отечественных продуктов не гарантирует хорошую работоспособность продукта, а только лишь соответствие продукта требованиям по информационной безопасности определенного уровня. В то же время, наличие отечественного сертификата у хорошо работающего иностранного продукта не гарантирует отсутствие в нем недекларированных возможностей (необходимо внимательно читать на что выдается сертификат) и иных интегральных уязвимостей. Самое главное от чего спасает наличие сертификата - это от замечаний при проверке федеральных органов.

Сайты основных регуляторов:

- ФСБ России (fsb.ru);
- ФСТЭК России (fstec.ru);
- Роскомнадзор (rsoc.ru).

Раздел 6

Используемые материалы

[1] Национальный стандарт Российской Федерации: «Практические правила управления информационно безопасностью». ГОСТ Р ИСО/МЭК 17799-2005. (Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. N 447-ст).

[2] Национальный стандарт Российской Федерации: «Защита информации. Основные термины и определения». ГОСТ Р 50922-2006.(Утвержден Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст Дата введения - 1 февраля 2008 года).

[3] Национальный стандарт Российской Федерации: «Информационная технология. Менеджмент услуг». ГОСТ Р 20000-2-2010 (Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 12 ноября 2010 г. N 381-ст).

[4] Федеральный закон «Об информации, информационных технологиях и о защите информации» N149-ФЗ от 27 июля 2006 года (Принят Государственной Думой 8 июля 2006 года).

[5] Национальный стандарт Российской Федерации: «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» ГОСТ Р ИСО/МЭК 27005-2010 (Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. N 632-ст).

[6] Национальный стандарт Российской Федерации: «Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности». ГОСТ Р ИСО/МЭК 27001-2006.(Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 375-ст).

[7] Руководящий документ: «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». (Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г).