УДК 681.3.067

О. А. Волков

РАЗРАБОТКА И АНАЛИЗ МОДЕЛИ ПОЛИТИКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ

Аннотация. Рассматривается модель политики безопасности компьютерной сети, позволяющая оптимизировать меры по защите информации. Оптимизация достигается за счет выделения групп защищаемых объектов.

Ключевые слова: защита информации, политика безопасности, компьютерная сеть.

Abstract. The article considers a model of computer network safety policy, allowing to optimize measures on information protection. The optimization is achieved through allocating groups of protected objects.

Key words: information protection, safety policy, computer network.

Введение

Обработка информации с помощью компьютерной техники в современном мире помогает решать практически любые задачи в различных сферах человеческой деятельности. Как правило, использование компьютеров становится более эффективным при объединении их в сеть. Это позволяет нескольким участникам объединять свои усилия для достижения общей цели. Компьютерные сети (КС) бывают разными: глобальная сеть Internet охватывает несколько континентов и служит платформой для огромного числа проектов, локальные сети могут ограничиваться объединением нескольких соседних квартир и использоваться для общения.

Однако использование сетевых технологий имеет ряд недостатков, к которым относится возможность несанкционированного доступа (НСД) к информации. Компьютерная сеть представляет собой комплекс программных и аппаратных средств, каждое из которых имеет уязвимости, дающие злоумышленнику возможность НСД. Роль злоумышленника может играть отдельное физическое лицо, действующее из хулиганских побуждений, или разведка иностранного государства. От личности злоумышленника зависят возможности по реализации тех или иных угроз, и ресурсы, которые могут быть задействованы для атаки.

Любая организация, решившая использовать КС в своей деятельности, должна осознавать возможность реализации угроз НСД и предпринять ряд мер для их нейтрализации. Для этого необходимо провести анализ обрабатываемой информации и отнести ее к определенной категории (например, информация, составляющая государственную тайну, персональные данные, данные, составляющие коммерческую тайну, или иные сведения, носящие конфиденциальный характер), разработать политики безопасности (ПБ) и, в соответствии с ними, внести необходимые корректировки в модель разрабатываемой КС.

Предлагаемая в данной работе модель ПБ позволит провести анализ и оценить возможность реализации тех или иных типов угроз на стадии планирования политик безопасности.

1. Анализ компьютерной сети

Как было сказано выше, КС представляет собой комплекс программных и аппаратных средств. Под аппаратными средствами подразумевается следу-

ющее оборудование: серверное (предназначенное для хранения и обработки больших массивов информации), оборудование технической защиты (криптомаршрутизаторы), персональные компьютеры (настольные, переносные), периферийное (принтеры, сканеры, источники бесперебойного питания, переносные носители информации), коммутационное (модемы, коммутаторы) и линии связи. Программные средства включают в себя прикладные и системные программы.

КС можно представить в виде узлов, объединенных линиями связи. Каждый такой узел может состоять из нескольких составляющих (программных и аппаратных). Чем больше узлов содержит сеть, тем больше вероятность успешной атаки на систему в целом, так как каждый узел подвержен риску угрозы НСД, а реализация одной из них на любом узле приведет к нарушению целостности системы в целом. В связи с этим не рекомендуется вводить избыточные узлы, узлы, которые не будут задействованы в обработке информации, а на самих узлах необходимо минимизировать количество компонентов. Например, удалить не используемые программы, учетные записи и снять неиспользуемое оборудование (Wi-Fi сетевую карту и т.п.).

Серверное оборудование является привлекательным объектом для злоумышленников. Обладая мощными вычислительными ресурсами, оно позволяет получить доступ к большим массивам обрабатываемой информации. Однако и защите такого оборудования обычно уделяется повышенное внимание. Программы для использования в серверах стоят дороже, их тестированию уделяется больше времени, что позволяет выявить большее число ошибок, приводящих к появлению угроз. Настройкой и эксплуатацией серверов занимаются подготовленные специалисты, что также снижает риск появления бреши в системе защиты. Немаловажным является и то, что устанавливают такое оборудование в помещении, защищенном от посторонних. Все это затрудняет действия преступников по успешной реализации атак.

Персональные компьютеры (ПК) сотрудников имеют гораздо больше уязвимостей. Целью атаки на них может быть как непосредственный доступ к ресурсам ПК, так и завладение узлом, посредством которого могут быть атакованы остальные части сети. В отличие от персонала, обслуживающего серверное оборудование, сотрудники, эксплуатирующие ПК, не всегда понимают риск, возникающий при совершении ими тех или иных действий. Установка непроверенного программного обеспечения, разглашение паролей, отключение антивирусов приводит к снижению уровня защищенности КС. С каждым годом во всем мире растет число инцидентов, связанных с потерей ноутбуков.

Во многих организациях использование периферийного оборудования не связывают с вопросами информационной безопасности, хотя сданный в ремонт ксерокс, хранящий в памяти последние распечатанные документы, или потерянная «флэшка» могут стать причиной НСД к конфиденциальной информации, что подтверждено опубликованными в общедоступных источниках инцидентами. Именно поэтому на этапе проектирования политик безопасности или при проведении реорганизации КС необходимо рассматривать угрозы, связанные с использованием периферийного оборудования наравне с остальными.

Каналы связи состоят из линий связи и узлов коммутации, в которых находится сетевое оборудование. В отличие от остальных узлов сети, каналы

связи часто подвержены несанкционированному воздействию (НСВ), не связанному с действиями злоумышленников. Деструктивные силы природного характера часто приводят к повреждению линий связи и выходу из строя коммутационного оборудования. Для минимизации последствий от такого НСВ должна быть предусмотрена возможность использования резервных каналов.

КС средних размеров включает в себя все эти элементы, каждый из которых приносит присущие ему уязвимости в общую структуру.

2. Разработка модели политики безопасности

Для надежной защиты системы необходимо, чтобы политики безопасности предусматривали все возможные угрозы и действовали во всех узлах. Разрабатывать единую политику безопасности для всех узлов КС нецелесообразно. Как показано выше, каждый узел имеет присущие ему уязвимости, следовательно, общая политика безопасности будет избыточной, что приведет к необоснованному ограничению функциональности данного узла. Существующие системы не являются статичными. Появление нового программного обеспечения и оборудования приводит к постепенному обновлению системы, а изменение требований к системе добавляет в нее новые элементы. Если политика безопасности общая для всех узлов, то изменения в системе постоянно будут приводить к изменению политик безопасности узлов, не подвергнутых изменению. В связи с этим целесообразно выявить группы узлов, для которых будет оправданным применение общей для них ПБ.

Выделение нескольких узлов в группу позволит установить правила поведения внутри группы и правила для взаимодействия с объектами вне группы. Соблюдение этих правил позволяет исключить внешнее несанкционированное воздействие. Полученный периметр можно считать защищенным. Защищенные периметры (ЗП) могут взаимодействовать на равных, как, например, несколько локальных групп пользователей, или входить один в другой, как локальная сеть, входящая в состав распределенной сети. В первом случае ПБ будут отличаться количественными параметрами (объемом общего дискового пространства, временем нахождения в сети), во втором случае – качественными (приоритетом одной ПБ перед другой).

Такой элемент сети, как персональный компьютер, не включает в себя других узлов, и в связи с этим его ЗП носит характер начального, базового уровня (рис. 1). Для построения защиты периметра базового уровня необходимо определить набор характеристик, соответствующих данной структурной единице. Название «персональный компьютер» подразумевает, что компьютер использует один человек, однако это не всегда так. Практически все современные операционные системы позволяют зарегистрировать на одном ПК несколько пользователей. Такая возможность очень важна для домашнего компьютера, где несколько человек в разное время используют один компьютер и хотят иметь личные данные, неприкосновенные для других, не говоря о персональных настройках интерфейса и т.п. Важна ли такая возможность для рабочего ПК? Безусловно, во-первых, это касается компьютеров, которые используют в несколько рабочих смен, когда один пользователь заканчивает работу, на его место приходит другой. Во-вторых, пользователь временно, например на период отпуска, передает ПК другому сотруднику. Существует практика, при которой несколько человек используют одну учетную запись,

но это, конечно, неправильно. Теряется возможность объективного мониторинга, невозможно отследить, кто конкретно какие действия совершал в системе, невозможно назначить разные права или наложить ограничения на пользователя. Также использование нескольких учетных записей на ПК необходимо при разграничении прав доступа к системе – в большинстве случаев на администратора и пользователя. Администратор обладает правами настраивать систему, устанавливать программное обеспечение, а пользователь имеет доступ лишь к области прикладных задач.

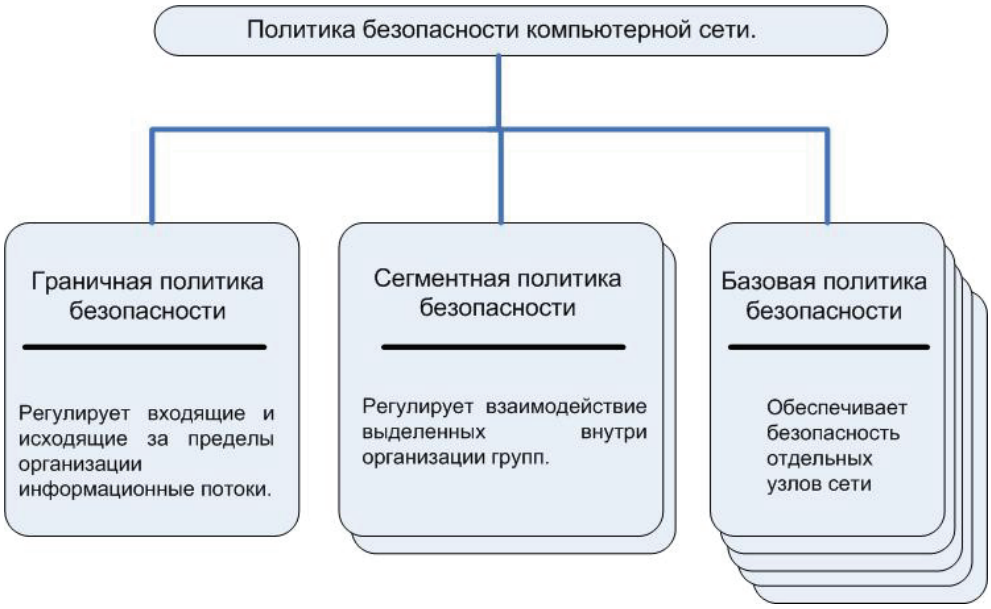

Рис. 1. Модель политики безопасности компьютерной сети

Наличие подключения рабочей станции к сети Internet значительно повышает шансы злоумышленника на успешную атаку. При подключении появляется риск получения злоумышленником несанкционированного удаленного доступа к ПК. Появляется риск инсайдерской атаки, направленной на хищение информации и передачу ее за пределы ЗП.

Переносные накопители информации приобретают все меньшие габариты, но все большую емкость данных. Появляется возможность незаметно внести или вынести большой объем информации. В связи с этим становится необходимо аппаратными и программными средствами ограничивать любое несанкционированное подключение устройств, способствующих хищению конфиденциальной информации.

Внутренняя угроза, исходящая от одного из сотрудников или группы лиц, направленная на хищение конфиденциальной информации, наиболее реальна и способна нанести огромный урон, так как может затронуть любую область информационных потоков организации. На этапе проектирования системы защиты невозможно определить, кто из членов организации решит воспользоваться служебным положением для получения личной выгоды. Кроме того, данный субъект, не имея прямого доступа к информации, может получить таковой, используя полученные обманным или иным способом идентификационные данные другого сотрудника (пароль, ключ доступа и т.п.).

Один из аспектов данной угрозы в том, что выявить потерю данных в короткие сроки практически невозможно, а значит, у злоумышленника остается достаточно времени распоряжаться полученной информацией по своему усмотрению.

Рынок индустрии информационных технологий предлагает в качестве решения данной проблемы установку так называемых DLP (Data Loss Prevention) систем – систем предотвращения потерь конфиденциальных данных. Данные системы включают в себя компоненты контекстного анализа на сетевых узлах и конечных хостах и компоненты, направленные на устранение возможности несанкционированного подключения оборудования. Однако использование таких систем ввиду ряда объективных причин не гарантирует безопасность. Сложность контекстного анализа в том, что даже специалист не может определить, насколько правомерно копирование информации за пределы организации. Информационные потоки изменяются, поэтому необходимо своевременное изменение параметров контекстного анализа, которое должен осуществлять специалист. Данный специалист должен досконально изучить работу всех отделов предприятия в части информационного обмена, отслеживать изменения и самостоятельно принимать решения по настройке DLP-системы. На практике осуществить это невозможно или невероятно трудно, даже если в роли специалиста будет выступать целое подразделение. Возложить принятие решений по циркуляции той или иной информации на структурные подразделения невозможно, во-первых, ввиду их заинтересованности; во-вторых, инсайдером может оказаться сотрудник, принимающий такие решения.

К данным проблемам стоит добавить реализацию системы предотвращения потерь, административные проблемы, связанные с соблюдением прав сотрудника на неприкосновенность частной жизни, и в результате получаем экономически затратную систему, которая не может гарантировать выполнение возложенных на нее функций по защите информации. Доверять такой системе опасно. Однако это не значит, что DLP-система вообще бесполезна. Как отмечалось выше, контроль за несанкционированной установкой оборудования может быть поручен такой системе. Кроме того, она может вести наблюдение и протоколировать события, касающиеся передачи данных для последующей обработки при расследовании инцидентов, а также обнаруживать явные нарушения, например попытку документа с грифом «секретно» покинуть пределы КС организации. Еще одна функция лежит в области социальной инженерии. Сотрудники, проинформированные о том, что в организации развернута DLP-система, и наблюдающие некоторые результаты ее работы, но не способные установить полноту защиты, будут склонны приувеличивать ее возможности и, как следствие, опасаться нарушать режим предприятия.

Выделение нескольких ПК в отдельную группу на основании схожих функциональных параметров (принадлежность к одному подразделению, обработка данных одного уровня конфиденциальности) позволяет назначить им ПБ, отличную от базовой. Она отвечает за взаимодействие ПК внутри данного сегмента и нескольких сегментов сети между собой (рис. 1).

Взаимодействие происходит посредством сетевых технологий. Основной угрозой становится захват злоумышленником одного из объектов либо внедрение ложного. Первоочередной целью системы защиты становится вы-

явление таких объектов. Фактором, позволяющим распознать злоумышленника, является аномальное, нетипичное поведение объекта. Подозрение может вызвать резкое увеличение сетевой активности, изменение графика активности, попытки внедрения или анализа и т.п. В большинстве случаев злоумышленник будет активно действовать в отношении соседних либо вышестоящих узлов.

Создание ПБ на базовом и сегментном уровнях позволит контролировать информационные потоки внутри КС. Информационный обмен с внешней средой должен быть регламентирован отдельной ПБ. Исходящие или входящие данные пересекают границу КС. Граничный уровень защиты наиболее подвержен риску, так как именно этот уровень напрямую связан с внешней средой (рис. 1). Именно этот уровень может быть подвержен случайным атакам – атакам, не направленным против данной организации. Внешняя среда является агрессивной сама по себе по причине полной открытости. Необходимо выявлять данные, не относящиеся к полезной информации, и блокировать им доступ в КС. Защита внешнего периметра носит двунаправленный характер. Должны быть предусмотрены отражение внешних атак и контроль за информацией, покидающей пределы организации. Часть рассмотренной выше DLP-системы настроена на предотвращение попыток копирования конфиденциальной информации за границы защищенного периметра организации.

Данные ПБ находятся в иерархической зависимости друг от друга. При перемещении данных через несколько уровней они будут подчинены ПБ более высокого уровня. Например, передача данных от ПК одной группы на ПК другой будет в первую очередь ограничена ПБ сегментного уровня, а после этого ПБ базового уровня (рис. 2).

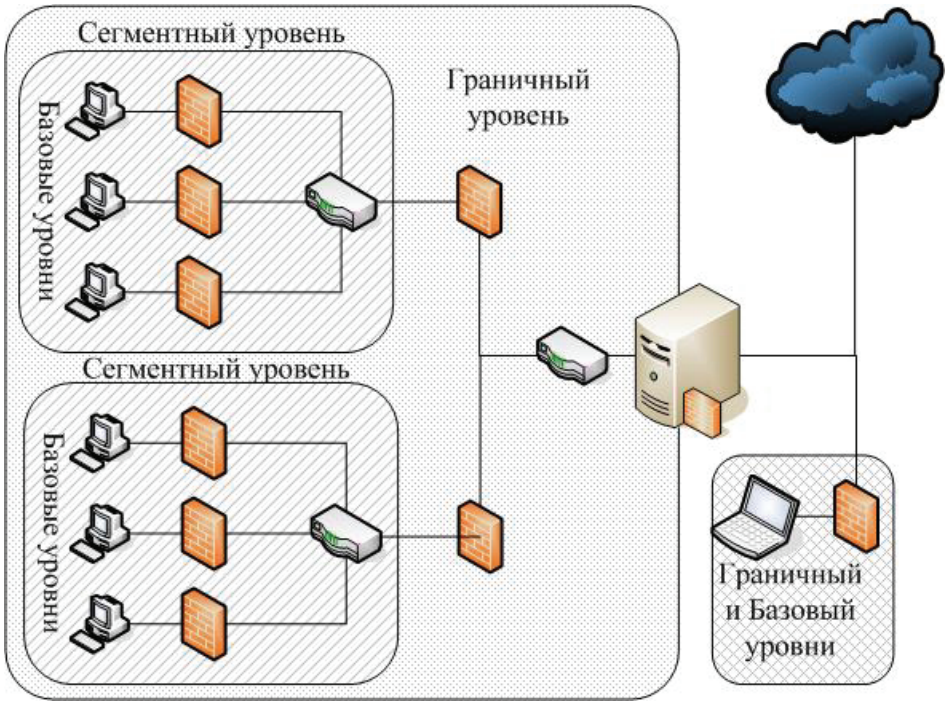

Рис. 2. Иерархия политик безопасности

Существуют ситуации, при которых ПБ граничного или сегментного уровня ограничивается одним узлом. ПК может входить в состав КС, но не быть членом группы, или это может быть удаленный ПК, отделенный сетью Internet от основной КС. В этих случаях иерархия не должна нарушаться, а ПБ должны составляться отдельно для каждого уровня. Так как, например, изменение требований организации к информационному обмену между группами не должно приводить к изменению ПБ на базовом уровне.

3. Анализ взаимодействия политик безопасности

Из изложенного понятно, что степень защищенности различных узлов системы не может быть одинаковой. А значит, и данные, обрабатываемые в этих узлах, будут подвержены разной степени риска несанкционированного воздействия. Разделив информацию по степени важности на несколько категорий, можно оптимизировать модель системы защиты любой организации. Цель оптимизации состоит в том, чтобы усилить защиту узлов, обрабатывающих более важную информацию, в связи с тем, что ее потеря нанесет большой урон предприятию. Наиболее действенным будет разделить данные на две группы: критические (данные, НСД к которым приведет к существенным потерям) и некритические. Дальнейшее дробление этих групп зависит от конкретных информационных потоков.

Основной принцип при проектировании системы защиты критических данных заключается в избыточности применяемых мер по защите. С одной стороны, необходимо усилить защиту узлов, на которых обрабатывается информация такого рода, с другой – запретить ее обработку на узлах, подверженных риску НСД. Проектируя защиту наиболее важных данных, необходимо учитывать все возможные угрозы: подбор персонала, проверку аппаратно-программных комплексов на наличие встроенных «закладок», пропускной режим в помещениях и т.п. Возможно, некоторые угрозы не удастся свести к минимуму, тогда их придется исключить. Например, отключить некий сегмент сети от глобальной сети на граничном уровне защиты, от остальной сети предприятия на сегментном и запретить использование переносных запоминающих устройств на нижнем, базовом уровне.

При передаче информации между различными участками КС возникают ситуации, требующие определить, какая из политик безопасности должна быть применена. Формализованный подход к данному вопросу позволит исключить возможность неоднозначного ответа и даст возможность программно обрабатывать возникшие противоречия. ПБ исходящего и входящего узлов должны иметь удельный вес (УВ), позволяющий при сравнении установить, какая из политик имеет приоритетное значение. Факторами, определяющими удельный вес ПБ, являются: уровень, на котором действует политика; степень важности информации, которую обрабатывает узел, подпадающий под действие данной политики. Сумма УВ этих факторов определяет УВ ПБ (табл. 1).

Таблица 1

Определение удельного веса политики безопасности

Степень конфиденциальности информации (УВ)	Уровень ПБ (УВ)		
	Базовый (1)	Сегментный (2)	Граничный (3)
Не критичная (1)	2	3	4
Критичная (2)	3	4	5

Диапазон УВ степени конфиденциальности может быть расширен в зависимости от требования конкретной организации. При совпадении весов должны быть соблюдены требования обеих ПБ.

Заключение

Система защиты КС организации представляет собой совокупность мер по детектированию и своевременному реагированию на возможные угрозы. Для повышения эффективности защиты информации следует разделить политику безопасности КС на несколько ПБ. Предлагается выделить три основных группы ПБ: базовая, сегментная и граничная. При анализе информационных потоков данные, потеря которых приведет к значительному ущербу для организации, необходимо выделять в отдельную группу, защите которой стоит уделить особое внимание. При передаче информации между узлами, регулируемыми разными ПБ, соблюдаются требования ПБ с большим удельным весом.

Список литературы

1. **Зайцев, А. П.** Техническая защита информации / А. П. Зайцев, А. А. Шелупанов, Р.В. Мещеряков. – М. : Горячая линия – Телеком, 2009. – 616 с.
2. **Клейменов, С. А.** Информационная безопасность и защита информации / С. А. Клейменов. – М. : Академия, 2007. – 336 с.
3. **Завгородний В. И.** Комплексная защита информации в компьютерных системах / В. И. Завгородний. – М. : Логос, 2001. – 264 с.
4. **Щеглов, А. Ю.** Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и Техника, 2004. – 384 с.

Волков Олег Алексеевич
аспирант, Ижевский государственный технический университет

Volkov Oleg Alekseevich
Postgraduate student,
Izhevsk State Technical University

E-mail: volkov-rus@yandex.ru

УДК 681.3.067

Волков, О. А.

Разработка и анализ модели политики безопасности компьютерной сети / О. А. Волков // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2011. – № 2 (18). – С. 38–45.