

1 Методология управления информационной безопасностью поставщиками информационных систем

В последнее десятилетие – период, когда произошло широкое распространение автоматизированных информационных систем, их объединение в единую глобальную сеть и массовое использование миллионами пользователей одних и тех же компонентов информационных систем (операционных систем, аппаратных платформ, протоколов обмена информацией), – большое значение приобрело то, как поставщики подобных универсальных платформ и компонентов (являющиеся иногда практически монополистами на определенных сегментах рынка) организуют работу по повышению уровня информационной безопасности по различным направлениям. Уровень влияния таких компаний на состояние дел в сфере информационной безопасности иногда может быть очень значительным – даже большим, чем международных организаций и некоторых правительственных структур.

Основные задачи организационной работы крупных (т.е. занимающих большую долю рынка) поставщиков широко используемых информационных систем в сфере информационной безопасности:

- закрепить свои рыночные позиции путем создания благоприятного имиджа в глазах покупателей и всего сообщества пользователей информационных систем;
- занять новые рыночные ниши, предъявляющие более строгие требования к уровню информационной безопасности по сравнению с массовым рынком (банковский сектор, правительственные структуры и др.);
- обеспечить эффективную интеграцию поставляемых продуктов в различные информационные системы и бизнес-процессы;
- избежать обвинений (в том числе и судебных исков) со стороны потребителей, чьи информационные системы могли бы подвергнуться атакам.

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

Приемы и методы управления информационной безопасностью на этом уровне в каждом случае могут быть различными и определяются для каждой компании-поставщика следующими основными факторами:

- характером продуктов, поставляемых на рынок;
- состоянием (конъюнктурой) рынка информационно-технологических продуктов такого типа и поведением конкурентов;
- политикой государственных структур как в отношении вопросов информационной безопасности вообще, так и в отношении отдельных компаний-поставщиков информационных систем, в частности;
- задачами, целями и основными способами использования поставляемых продуктов пользователями;
- общим состоянием дел в сфере информационной безопасности, информационной культурой, развитием и распространением преступности;
- формируемым общественным мнением в отношении вопросов информационной безопасности и отдельных компаний-поставщиков.

Организационная работа в сфере информационной безопасности на уровне таких компаний разделяется на два основных под-направления:

- организация работы внутри компаний, специально направленной на обеспечение информационной безопасности выпускаемых продуктов;
- организация внешнего взаимодействия с потребителями, партнерами, государственными структурами и другими участниками.

Внутренняя организационная работа по обеспечению информационной безопасности производимых и продаваемых продуктов является неотъемлемой частью процесса проектирования, производства и маркетинговой поддержки этих продуктов. Однако при этом выделяются дополнительные специальные мероприятия, осуществляемые отдельно от основных производственно-сбытовых процессов в компаниях – крупных производителях информационных систем. Примерами таких специальных

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

организационных мероприятий является создание специальных подразделений, чьей основной задачей является контроль за устранением существующих уязвимостей и выполнение сопутствующих функций, а также обучение разработчиков специальным методам разработки программного обеспечения и аппаратных средств, не содержащих уязвимостей.

Основные приемы и методы внешней организационной работы в сфере информационной безопасности на уровне крупных компаний–поставщиков информационных систем могут быть следующие:

- организация информационного обмена с пользователями выпускаемых продуктов – программных и аппаратных средств (информирование о выявленных уязвимостях и способах их устранения, получение информации об уязвимостях, выявленных пользователями, а также других возникающих проблемах);

- организация деятельности в сфере подготовки специалистов (система подготовки квалифицированного инженерно-технического персонала, специализирующегося на определенных программных продуктах и, в частности, на администрировании средств защиты информации, сетевых операционных систем и т.п.);

- организация профессиональных конференций, которые способствуют обмену опытом и информацией, связанной с повышением уровня информационной безопасности при использовании определенных программных и аппаратных платформ;

- организация взаимодействия с правительственными организациями (в том числе по вопросам сертификации программных и аппаратных средств на соответствие требованиям национальных стандартов и правил);

- создание и поддержание системы сертификации специалистов, ориентированной на определенные программные продукты и аппаратные системы (в том числе, организация взаимодействия со специализированными

компаниями, занимающимися профессиональным тестированием специалистов и др.).

Организация информационного обмена с пользователями продуктов является одним из наиболее важных направлений деятельности компаний в данной сфере. Эта работа включает в себя сбор информации, ее анализ, а также принятие решений о том, необходимо ли информировать все сообщество пользователей, которых может коснуться выявленная уязвимость, или только ограниченный круг доверенных специалистов, имеющих необходимые полномочия и авторитет. Дальнейшие действия, как правило, связаны с уведомлением пользователей о возможных способах решения проблем (потенциальных или уже возникших) и информированием о возможных последствиях реализации угроз.

2 Управление информационной безопасностью поставщиками информационных систем

2.1 Корпорация Microsoft

Корпорация Microsoft является крупнейшим в мире производителем программного обеспечения – ее программные продукты распространены по всему миру. В частности, Microsoft производит и поставляет следующие основные программные средства:

- операционные системы для рабочих станций (пользовательских персональных компьютеров) семейства Windows;
- операционные системы для сетевых серверов (веб-серверов, серверов баз данных, файл-серверов и др.) – старшие версии операционных систем семейства Windows;
- операционные системы для мини-компьютеров (PDA) – семейства Windows CE и Windows Pocket PC;
- специализированные функциональные серверы: серверы реляционных баз данных (Microsoft SQL Server), веб-серверы (IIS – Internet

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

Information Server), системы построения хранилищ данных (Analysis Services) и некоторых других;

- средства разработки приложений;
- пользовательские программные продукты для платформы Windows: веб-браузеры, почтовые клиенты, программы верстки в формате HTML, офисные приложения, мультимедийные приложения и другие.

Также корпорацией Microsoft была приобретена компания, занимающаяся поставками систем управления предприятиями (систем класса ERP – Enterprise Resource Planning).

В силу того, что программными продуктами Microsoft пользуется большинство пользователей персональных компьютеров (как частных, так и в коммерческих и правительственных организациях), а на основе серверных программных платформ Microsoft функционирует большинство информационных систем, обеспечивающих обработку, хранение и передачу информации (в том числе и в сети Интернет), организационная работа этой корпорации в сфере информационной безопасности имеет глобальное значение.

Внутренняя организационная работа в сфере информационной безопасности продуктов корпорации Microsoft включает в себя:

- проведение специальных тренингов и дополнительного обучения разработчиков программного обеспечения специальным методам, обеспечивающим надежность и безопасность производимого программного обеспечения (включая внедрение и использование для разработки собственных продуктов методологии Жизненного цикла безопасной разработки);
- организацию специального Центра решения вопросов безопасности (Microsoft Security Response Center, MSRC), основными задачами которого являются постоянный сбор информации и поиск новых уязвимостей, принятие

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

мер к устранению выявленных уязвимостей, координация работы разработчиков и недопущение появления ранее выявленных уязвимостей в новых продуктах в будущем.

В организационной структуре Microsoft помимо MSRC существуют еще одно подразделение, специализирующееся на решении вопросов безопасности – Центр защиты от вредоносных программ (Microsoft Malware Protection Center, ММРС). Он включает в себя несколько лабораторий, расположенных по всему миру, и занимается исследованием вредоносных программ, обеспечивает методическую поддержку разработки различных средств защиты (таких, как Windows Live OneCare, Windows Defender, Malicious Software Removal Tool), а также участвует в процедурах реагирования на возникновение новых угроз безопасности.

Основными направлениями внешней организационной работы корпорации Microsoft в сфере информационной безопасности являются:

- систематическое информирование пользователей операционных систем Windows (а также других программных продуктов) о выявленных уязвимостях и распространение информации о том, как эти уязвимости могут быть ими устранены;
- реализация программы упреждающих защитных действий – Microsoft Active Protections Program (MAPP);
- поддержка обучения пользователей программных продуктов (в основном администраторов серверных платформ);
- разработка и поддержка методологии Жизненного цикла безопасной разработки – Microsoft Security Development Lifecycle (SDL);
- партнерская программа Microsoft Security Partners – Партнеры Microsoft в сфере безопасности;
- Government Security Program (GSP) – Программа обеспечения безопасности правительств;

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

- организация конференций по различным аспектам использования программных продуктов Microsoft;
- организация специального фонда для борьбы с хакерами;
- организация централизованной сертификации своих продуктов в государственных органах;
- проведение собственной конференции по безопасности.

1) Организация информирования пользователей о выявленных уязвимостях – строится на основе т.н. Бюллетеней Безопасности ("Security Bulletin"), выпускаемых с определенной периодичностью, а также по мере выхода специальных обновлений, устраняющих выявленные уязвимости (т.н. "заплат", patches). Порядок выпуска этих бюллетеней, их содержание и другие вопросы регулируются специальным организационным документом – Процедурой Выпуска Бюллетеней Безопасности (Security Bulletin Release Process). Также в рамках этой работы организован сбор информации об уязвимостях, выявляемых пользователями: на Интернет-сайте компании размещена специальная форма, заполнив которую, каждый желающий может сообщить о новых самостоятельно обнаруженных уязвимостях в программных продуктах.

2) Программа упреждающих защитных действий – Microsoft Active Protections Program (MAPP) – представляет собой систему ускоренного информирования разработчиков систем безопасности (антивирусов, систем обнаружения и предотвращения вторжений) о вновь выявленных уязвимостях. Данная программа реализуется для того, чтобы сторонние разработчики систем безопасности могли не дожидаться выхода очередного Бюллетеня Безопасности и как можно раньше начать разрабатывать механизмы нейтрализации новых уязвимостей на основе своих программных решений. Для участия в данной программе допускаются разработчики систем защиты на

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками
информационных систем
(Планирование и управление информационной безопасностью)

основе программных платформ Microsoft, клиентская база которых составляет не менее 10000 пользователей.

3) Поддержка системы обучения пользователей и администраторов реализуется несколькими основными способами:

- целенаправленная подготовка и опубликование учебных пособий, справочников, статей и других учебных материалов, содержащих пояснения, пошаговые инструкции, примеры конфигурации и сценарии для установки программных продуктов, в том числе и такие, которые должны обеспечить решение вопросов информационной безопасности;

- организация и методическая поддержка системы профессионального обучения и сертификации специалистов по различным программным продуктам (в том числе администраторов сетевых операционных систем, баз данных и других серверных продуктов, таких как Internet Security and Acceleration Server). Такая поддержка включает в себя сертификацию преподавателей учебных центров, сертификацию самих учебных центров, а также установление партнерских отношений с организациями, занимающимися профессиональным обучением и профессиональным тестированием администраторов и разработчиков информационных систем;

- проведение бесплатных семинаров для администраторов операционных систем, посвященных вопросам обеспечения информационной безопасности (в частности, функциональным возможностям тех или иных программных продуктов, обеспечивающим решение определенных вопросов защиты информации).

4) Одним из направлений информационной и методической поддержки сообщества специалистов является продвижение и популяризация среди разработчиков информационных систем методологии Жизненного цикла безопасной разработки – Microsoft Security Development Lifecycle (SDL). Данная методология представляет собой набор универсальных методических,

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками информационных систем
(Планирование и управление информационной безопасностью)

технических и организационных рекомендаций и приемов, в совокупности обеспечивающих существенное повышение уровня безопасности разрабатываемого ПО. Так, по утверждению Microsoft, после внедрения данной методологии ей удалось снизить общее число уязвимостей, выявленных в SQL Server в течение трех лет после выпуска продукта на рынок, на 91% (если в MS SQL 2000 было выявлено 34 уязвимости, то в MS SQL 2005 – всего 3 уязвимости).

Продвижение данной методологии в среде разработчиков информационных систем включает в себя:

- опубликование и постоянное развитие самой методологии;
- организацию профессионального сообщества (SDL Pro Network), которое объединяет консалтинговые компании и учебные центры, специализирующиеся на вопросах безопасности;
- разработку и распространение шаблонов для среды разработки Visual Studio, поддерживающих выполнение положений методологии.

5) Microsoft Security Partners – программа построения партнерских отношений с различными независимыми компаниями, работающими в сфере информационной безопасности. Данная программа развивается по нескольким самостоятельным направлениям:

- Antivirus Partners – Партнерство в создании антивирусных и защитных программ, а также в обмене актуальной информацией о новых вирусах, воздействующих на различные продукты Microsoft. В этой программе участвуют такие фирмы, как Symantec, ДиалогНаука, Лаборатория Касперского, Panda Software и другие (всего около 20 различных компаний);
- Альянс SecureIT – партнерство с разработчиками решений в сфере безопасности (VeriSign, Trend Micro, Symantec и др.) по совместной разработке новых средств в данной области. Члены альянса получают от Microsoft и друг

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками
информационных систем
(Планирование и управление информационной безопасностью)

от друга закрытую информацию о новых разработках, позволяющую создавать интегрируемые и взаимодействующие решения;

- ISA Server Partners – партнерство с разработчиками программных и аппаратных решений, адаптированных для платформы Internet Security and Acceleration Server;

- Microsoft Windows Rights Management Services Partners – Партнерство с компаниями-разработчиками программных продуктов, разработчиками аппаратных средств идентификации и системными интеграторами в вопросах более полного использования функциональных возможностей ОС Windows, связанных с управлением правами пользователей и доступом к информационным ресурсам. Данная программа включает в себя три категории партнеров: Независимых поставщиков ПО, Разработчиков инфраструктурных решений и Системных интеграторов.

6) Government Security Program (GSP) – Программа обеспечения безопасности правительств – представляет собой инициативу по передаче правительственным структурам различных стран исходных кодов программных продуктов (главным образом, операционных систем) для того, чтобы у специалистов и экспертов была возможность убедиться в отсутствии существенных изъянов в этом программном обеспечении. Такой анализ должен дать основания для признания этих программных продуктов надежными с точки зрения информационной безопасности и, таким образом, расширить возможности их применения различными организациями (как правительственными, так и частными). Также предполагается, что эта программа должна помочь устранить имеющиеся недоработки в программном обеспечении и расширить партнерство между Microsoft и правительствами различных стран в сфере защиты информации. В рамках программы участвующим в ней экспертам также предоставляется доступ к документации, справочные материалы, специальные средства для работы с исходными

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками
информационных систем
(Планирование и управление информационной безопасностью)

кодами и поддержка со стороны специалистов Microsoft. В данную программу включены около 60 стран (в том числе и Россия в лице ФСТЭК), отвечающих определенным требованиям к защите прав на интеллектуальную собственность.

Одной из возможных причин начала реализации этой программы явилось то, что некоторые правительства (например, Германии) заявили о возможном переходе правительственных и муниципальных учреждений на альтернативные операционные системы (такие как, например, Linux), для которых доступны исходные коды. Развитие этой тенденции в перспективе могло привести (и отчасти уже привело) к определенной потере рынков сбыта продукции Microsoft.

7) Централизованная сертификация программных продуктов в государственных органах является для корпорации Microsoft одним из направлений реализации концепции развития защищенных информационных систем и предполагает возможность использования программного обеспечения этой компании в информационных системах, к которым предъявляются особые требования с точки зрения надежности и информационной безопасности. Так, сертификация ФСТЭК операционных систем и систем управления базами данных, поставляемых Microsoft, позволила использовать эти программные продукты в автоматизированных системах учета и контроля ядерных материалов на предприятиях Минатома РФ и в других организациях. Первый проект по сертификации продуктов Microsoft в России был начат в 1996 году и продолжался на протяжении примерно трех лет с участием не только специалистов Гостехкомиссии РФ и Microsoft, но и представителей Минатома РФ и Министерства энергетики США. Также Microsoft ведет работу по сертификации некоторых своих продуктов на соответствие стандарту Common Criteria for Information Technology Security Evaluation – универсальному стандарту обеспечения

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками
информационных систем

(Планирование и управление информационной безопасностью)

информационной безопасности, официально признаваемому многими государствами.

Конференция по безопасности BlueHat проводится с 2005 года дважды в год для обмена мнениями и идеями по различным вопросам информационной безопасности. В ней участвуют только специалисты, приглашаемые компанией Microsoft.

2 Корпорация Cisco Systems

Компания Cisco Systems, основанная в 1984 году группой специалистов Стэнфордского университета, в настоящее время является мировым лидером в производстве оборудования для сетей передачи данных. На основе оборудования, произведенного этой компанией, функционируют глобальные сети передачи данных, а также сети многих правительственных организаций и крупных компаний.

В связи с тем, что оборудование этой компании обеспечивает функционирование большинства наиболее значимых и ответственных сетей передачи данных, ее организационная поддержка решения вопросов информационной безопасности имеет глобальное значение.

В число основных направлений организационной работы компании Cisco входят:

- поддержка сети образовательных центров – Сетевая Академия Cisco – при различных учебных учреждениях и предприятиях. Работа Сетевых Академий по всему миру обеспечивает подготовку специалистов по администрированию сетей и обеспечению сетевой безопасности и централизовано поддерживается головным офисом, который осуществляет подготовку преподавателей, предоставляет учебные материалы, ведет учет слушателей, осуществляет экзаменационное тестирование выпускников, выписывает международные сертификаты и т.д. В России функционирует более 50-ти Сетевых Академий Cisco;

- организация и координация работы поставщиков различных компонентов информационной инфраструктуры на основе программы Network Admission Control (NAC) – Управление Доступом в Сеть. В рамках данной программы, инициированной в 2020 году совместно с ведущими поставщиками антивирусов (Network Associates, Symantec и Trend Micro) и нацеленной на решение различных проблем информационной безопасности,

Тема 3.3 – Планирование и управление информационной безопасностью поставщиками
информационных систем
(Планирование и управление информационной безопасностью)

Cisco планирует реализовать новые технические решения и подходы к обеспечению информационной безопасности, основанные на собственном сетевом оборудовании. В частности, кооперация с поставщиками программных продуктов в рамках данной программы должна позволить автоматически управлять подключением компьютеров, не отвечающих определенным требованиям (политикам) информационной безопасности;

- организация работы Cisco Product Security Incident Response Team (PSIRT) – Группы реагирования на инциденты, связанные с безопасностью продуктов Cisco. Основной задачей этого подразделения является сбор информации о выявленных уязвимостях, их анализ, а также координация работ по их устранению и предотвращению негативных последствий;

- распространение информации о выявленных уязвимостях и проблемах с безопасностью.