ПОСТРОЕНИЕ МНОГОУРОВНЕВОЙ АНТИВИРУСНОЙ ЗАЩИТЫ НА ПРИМЕРЕ ФИНАНСОВОЙ ОРГАНИЗАЦИИ

А.А. Пирогов
Алтайский государственный университет, г. Барнаул

Развитие вредоносного программного обеспечения (ПО) произошло после создания финансовых потоков в информационно-телекоммуникационных сетях связи. В связи с этим наибольшими объектами атак вредоносного ПО все чаще становятся банки и финансовые организации. Если банк имеет средства для внедрения современных решений противовирусных систем защиты информации (СЗИ), то финансовые организации, зачастую, лишены такой возможности из-за сложности таких технологий и больших финансовых затрат на интеграцию СЗИ в имеющуюся информационную инфраструктуру (ИИ). Описанные выше проблемы заставляют финансовые организации использовать более низкий класс СЗИ, тем самым повышая риск вирусной атаки. Целью данной работы является построение противовирусной защиты с применением Российских и международных стандартов на примере организации ООО «Финансист».

Вредоносное программное обеспечени (ВПО) – ПО, разработанное злоумышленником, целью которого является нанесение ущерба владельцу информации, либо несанкционированное использование ресурсов ЭВМ. Согласно классификации ФСТЭК вредоносные программы делятся на [1]: программные закладки типа «троянский конь»; программный вирус; сетевые черви; вредоносные программы, обеспечивающие осуществление НСД. В зависимости от места расположения и алгоритма работы ВПО могут быть реализованы различные скрытые способы, которые делятся на нетрадиционные информационные каналы (используется ПАЗ) и скрытые каналы (используется ПВМ). Опасность скрытых каналов основана на предположении постоянного доступа нарушителя безопасности к ИО организации взаимодействия через эти каналы на ИС [1] для нанесения максимального ущерба организации (рис. 1).

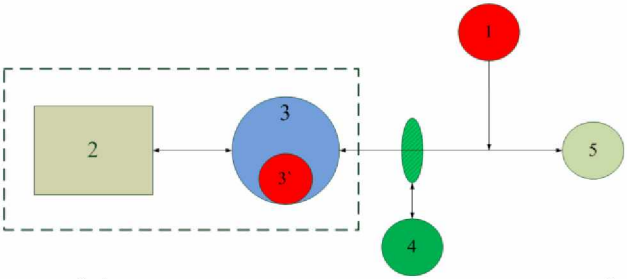

Рис. 1. Общая схема взаимодействия вредоносного ПО с нарушителем, посредством СК.

На схеме присутствуют следующие компоненты: 1 - нарушитель безопасности (злоумышленник); 2 - информация ограниченного доступа; 3 - субъект, имеющий санкционированный доступ к 2 и 5; 3' - агент нарушителя безопасности, находящийся в замкнутом контуре с 2 и взаимодействующий с 2 от имени субъекта 3; 4 - инспектор (программное средство), контролирующий(ее) информационное взаимодействие 3, пересекающее замкнутый контур, отделяющий объект информатизации от внешней среды; 5 - субъект, находящийся вне замкнутого контура, с которым 3 осуществляет санкционированное информационное взаимодействие.

Для успешного функционирования вредоносного ПО в информационной системе (ИС) необходимо присутствие определенных компонентов, а именно: устройство; операционная система; приложения. Для понимания специфики атаки вредоносного ПО была создана модель Cyber-Kill Chain (рис. 2) [2].

Рис. 2. Схема реализации воздействий, исходящих от вредоносного ПО согласно модели Cyber-Kill Chain.

Антивирусная защита (АВЗ) – защита информации и компонентов информационной системы (ИС) от ВПО. Средство антивирусной защиты (САВЗ) – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации СЗИ, а также реагирования на обнаружение этих программ и информации.

Несколько САВЗ, разного типа и назначения называются системой антивирусной защиты или многоуровневой антивирусной защитой. Любая информационная система состоит из нескольких классов компонентов, которые требуют защиты от вредоносных программ. Они делятся на три основных уровня: уровень шлюза; уровень серверов; уровень рабочих станций. Все САВЗ имеют определенный набор функций, в зависимости от цели реализации АВЗ и ИТ, для которых они предназначены. Класс и тип САВЗ выбирается исходя из класса ИСПДн и предъявляемых требования в соответствии с классом и категорией информации, обрабатываемой ИСПДн.

Информационные потоки организации подразумевают взаимодействие с юридическими (ЮЛ) и физическими лицами (ФЛ). Между ЮЛ, ФЛ и организацией происходят социальные правоотношения, подкрепляемые договорами различного направления. Такие договоры требуют заполнение реквизитов ЮЛ и персональных данных ФЛ согласно ст. 806 Гражданского кодекса. Краткая характеристика информационной системы ПРЕДПРИЯТИЯ приведена в таблице 1.

Таблица 1. Краткая характеристика ИСПДн

Описание характеристики	**Сведения об ИС**
Наименование ИСПДн	«Финансист»
Количество автоматизированных рабочих мест в ИСПДн.	До 50
Категория обрабатываемых в информационной системе ПДн	Иные - ПДн не являющимися специальными, биометрическими и общедоступными.
Количество субъектов ПДн, ПДн которых будут обрабатываться в ИС	Более 100 000
Характеристики безопасности ПДн	Требуется выполнение требований ФСТЭК
Структура ИСПДн	Локальная ИС
Тип ИСПДн	ИС, обрабатывающая иные категории ПДн
Наличие подключений к сети «Интернет»	ИС имеет подключения к сети «Интернет».
Режим обработки ПДн	Однопользовательский
Размещение технических средств	Все технические средства находятся на территории РФ
Режим разграничения прав доступа	Без разграничения прав доступа

Доступ к базе данных 1С осуществляться по персональному логину и паролю, выданному всем перечисленным выше сотрудникам. Доступ к серверу, на котором хранится база данных 1С, может осуществляться всеми сотрудниками организации. Объектами атаки в данному случае является база данных 1С, сервер с базой данных 1С и АРМ сотрудников, имеющих доступ к базе данных 1С и серверу 1С. Структура ИС приведена на рис. 3.

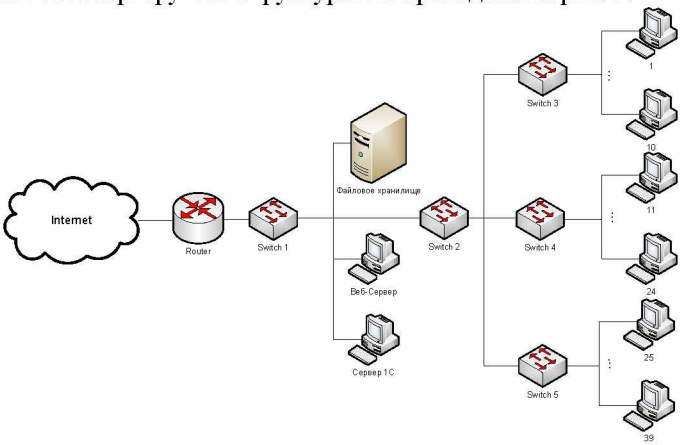

Рис. 3. Структура ИС организации.

Рис. 3 показывает особенности структуры ИС. Текущая структура ИС содержит потенциальные уязвимости в архитектуре, так как не весь трафик может проходить через средства фильтрации только на уровне логической архитектуры. В случае сбоев в работе оборудования или ошибок, допущенных администратором, вредоносных трафик может быть доставлен любому узлу сети [3].

В результате проведенного анализа что персонал и приложения имеют потенциальный доступ ко всем ресурсам организации и сети «Интернет», а любые операции с ПДн и КИ и сама инфраструктура не имеют какой-либо потенциальной защиты (рис. 4).

Анализ АРМ с помощью ПО «AIDA 64», «Anvir», «Defacto» показал, что средний показатель установленного ПО единообразен, но в виду отсутствия ограничения на установку ПО, пользователи устанавливали дополнительное ПО, зачастую устанавливая дополнительные компоненты в автоматическом режиме, что вело к неконтролируемому росту ПО на АРМ. Средний показатель установленного пиратского ПО на АРМ равен 10 %; ПО отстающее

от актуальной копии на 2 и более версии – 3 %; ПО, содержащее высокие и критические уязвимости – 5 % [1].

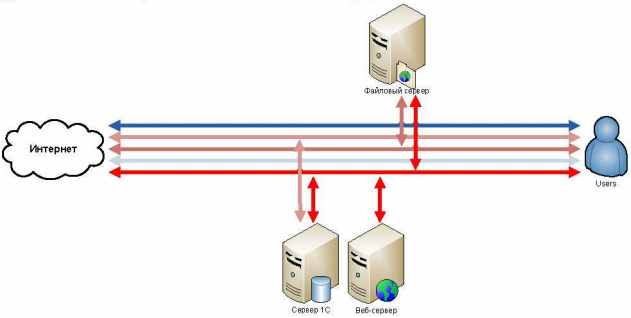

Рис. 4. Схема потоков данных в ИС

Конфигурация безопасности АРМ организации проверялась с помощью программного обеспечения MBSA v. 2.3, а оценка рисков организации производилась с помощью программного обеспечения MSAT v 4.0. Оценка риска производится по двум основным факторам: профиле риска для бизнеса (ПРБ) и индекса эшелонированной защиты (DiDI). Критерии анализа идут по двум основным направлениям [4, 5]: вопросы о бизнес-модели организации; вопросы применения мер защиты.

Итоговая оценка рисков распределяется на 4 направлениям: инфраструктура; приложения; операции; персонал. Сравнительный анализ рисков организации и технологий защиты показал большую разницу в числовых показателях (рис. 5).

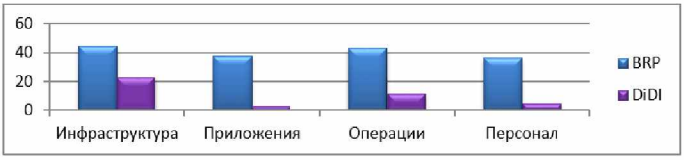

Рис. 5.Сравнительный анализ рисков и технологий защиты

В результате проведенного исследования анализ показал, что все четыпе направления имеют высокий уровень опасности, а уровень исходной защищенности ИС определяется как средний (Y1 = 5), так как не менее 70% характеристик ИС соответствуют уровню не ниже «средний», а анализ угроз атаки вредоносных

программ показал «высокий» уровень вероятности. Что делает данные угрозы «актуальными».

Исследование иностранной технической документации показало, что актуальную модель многоуровневой системы защиты показали руководства компаний-производителей технического и программного обеспечения (*руководство Microsoft по многоуровневой антивирусной защите)*.

Анализ рынка готовых антивирусных решений, разрешенных ФСТЭК, показал две компании-производителя, предоставляющие сертифицированные САВЗ (Касперсткий и Др.Веб). Произведенных анализ существующий решений и описанный выше документации позволил выдвинуть две концепции антивирусной защиты:

1) создание САВЗ на основе готовых антивирусных решений;

2) создание САВЗ на основе рекомендаций компаний-производителей используемых ИТ-решений (Mocrosoft).

Итоговый финансовый анализ двух концепций отдал предпочтение концепции на основе рекомендаций компании-производителей в виду более низких финансовых затрат (Касперский – 148 000 р.; Др.Веб – 156 000 р.; Microsoft – 69 000 р.). Первым уровнем построения антивирусной защиты (уровень шлюза) стало изменение схемы сети, с целью пропуская сетевого трафика через узел, выступающий в виде фильтра сетевого трафика (рис. 6).

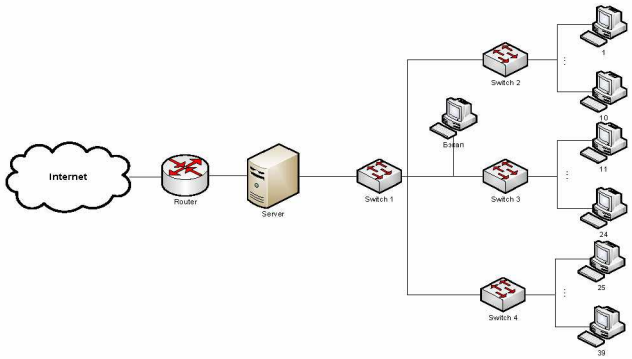

Рис. 6. Модернизированная структура сети.

Вторым этапом (уровень серверов) произведена настройка работы сервером согласно представленной рекомендации (рис. 7).

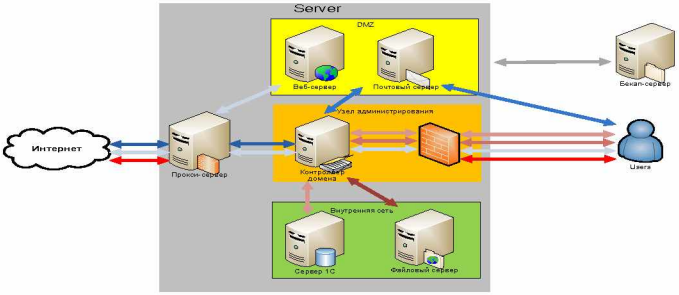

Рис. 7. Диаграмма потоков данных после модернизации.

Последним этапом (защитой АРМ) была подготовка рабочих станций [5]. Процесс внедрения САВЗ дал возможность выполнить следующие показатели:

– нейтрализовать вредоносное ПО (*178 объектов*);

– устранить пиратское ПО (*снизить на 10 %*);

– устранить уязвимое ПО (*снизить на 5 %*);

– устранить устаревшее ПО (*снизить на 3 %*);

– настроить политику безопасности на АРМ и серверах;

– разработать документы по политике антивирусной защиты и регламенту по антивирусному контролю.

Таким образом, проведенный комплекс мероприятий позволил:

– снизить уровень опасности актуальных угроз (в среднем с 0,8 до 0,2) снизив уровень с высокого до низкого, сделав их неактуальными;

– повысить уровень защиты объекта от вредоносного ПО с низкого до высокого, тем самым актуализировав многоуровневую антивирусную защиту.

Библиографический список

1. Руководство по многоуровневой антивирусной защите. [Электронный ресурс]: Microsoft – Режим доступа: https://technet.microsoft.com/ru-ru/library/cc162791.aspx – Загл. с экрана.

2. Что такое Cyber-Kill Chain и почему ее надо учитывать в стратегии защиты [Электронный ресурс] – Режим доступа: https://habr.com/company/panda/blog/327488/– Загл. с экрана.

3. Методические рекомендации по составлению частной модели угроз безопасности персональных данных при обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости (утв. Министерством здравоохранения и социального развития РФ 23 декабря 2009 г.) – 213 с.
4. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (утв. Министерством здравоохранения и социального развития РФ 23 декабря 2009 г.) – 226 с.
5. Настройка базовой конфигурации безопасности [Электронный ресурс]: Microsoft – Режим доступа: https://technet.microsoft.com/ru-ru/library/ee914623.aspx – Загл. с экрана.