Воронежский институт МВД России

Кафедра информационной безопасности

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИСОД МВД РОССИИ

Методические рекомендации

Воронеж 2019

ББК

Рассмотрено и одобрено на заседании кафедры информационной безопасности, протокол № от 2019 г.
Рассмотрено и одобрено на заседании методического совета, протокол № от 2019 г.

Авторский коллектив: О.И. Нестеровский, С.В, Зарубин, Д.Ю. Лиходедов.

Рецензенты:
Е.А. Рогозин – профессор кафедры автоматизированных информационных систем ОВД, д.т.н., профессор.
В.В. Довгань – Начальник отдела защиты информации ЦИТСиЗИ ГУ МВД России по Воронежской области, подполковник внутренней службы.

Управление инцидентами информационной безопасности в ИСОД МВД России: методические рекомендации [Электронный ресурс] / О.И. Нестеровский [и др.]. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2019. – 1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

В методических рекомендациях рассматриваются понятие инцидента информационной безопасности, процедуры управления инцидентами, особенности их анализа. Описывается программно-технических комплекс предупреждения и обнаружения инцидентов информационной безопасности в компьютерных сетях «СОПКА».
Пособие предназначено для слушателей радиотехнического факультета, обучающихся по специальности 10.05.02 Информационная безопасность телекоммуникационных систем, а также для использования в практической деятельности сотрудников подразделений по технической защите информации МВД России.

ISBN 978-5-88591-246-4

СОДЕРЖАНИЕ

ВЕДЕНИЕ

В настоящее время в телекоммуникационной системе МВД России обозначилась особая потребность в построении полноценной комплексной системы обнаружения, реагирования и предупреждения возникновения инцидентов информационной безопасности. В основе принципов работы такого механизма лежит система защиты от утечек информации, которая основывается в том числе на выявлении, предотвращении, регистрации и устранении последствий инцидентов информационной безопасности или событий, нарушающих регламентированные процедуры защиты. Существует ряд методик, определяющих основные параметры управления ими. Эти методики внедряются на уровне международных стандартов, устанавливающих критерии оценки качества менеджмента в компании. События или инциденты информационной безопасности в рамках этих регламентов выявляются и регистрируются, их последствия устраняются, а на основании анализа причин их возникновения положения и методики дорабатываются.

Актуальность проведения научно-исследовательской работы заключается в недостаточной проработке вопросов построения комплексной системы обнаружения, реагирования и предупреждения возникновения инцидентов безопасности. Проблема, на решение которой направлено научное исследования – необходимость проведения углубленного анализа особенностей построения системы управления инцидентами безопасности в ИСОД МВД России.

Целью исследования является анализ подходов к управлению инцидентами безопасности в ИСОД МВД России. Для выполнения данной цели в научно-исследовательской работе *решены следующие задачи*: описано понятие и типы инцидентов информационной безопасности, определено место системы управления инцидентами информационной

безопасности в общей группе механизмов защиты информации, проанализированы особенности управления событиями безопасности в ИСОД МВД России, предложены рекомендации по установлению причин и анализу последствий реализации инцидентов информационной безопасности.

Результаты научно-исследовательской работы обобщены в методических рекомендациях, которые планируются внедрить в образовательный процесс Воронежского института МВД России при изучении таких дисциплин, как «Информационная безопасность телекоммуникационных систем», «Компьютерная разведка», «Защита информации в вычислительных сетях», «Защита инфокоммуникационных сетей специального назначения» и других.

Методические рекомендации полезны также практическим сотрудникам территориальных органов МВД России, занимающихся вопросами обеспечения информационной безопасности объектов информатизации ОВД.

1 Особенности проявления инцидентов информационной безопасности в ИСОД МВД России

1.1 Понятие инцидента информационной безопасности

Международные регламенты, действующие в сфере сертификации менеджмента информационных систем, дают свое определение. Применительно к телекоммуникационной системе ОВД и согласно этим регламентам инцидентом информационной безопасности является единичное событие нежелательного и непредсказуемого характера, которое способно повлиять на процессы в ИСОД МВД России, скомпрометировать их или нарушить степень защиты информационной безопасности. На практике к этому понятию относятся разноплановые события, происходящие в процессе работы с информацией, существующей в электронной форме или на материальных носителях. К ним может относиться и оставление документов на рабочем столе в свободном доступе для другого персонала, и хакерская атака – оба инцидента в равной мере могут нанести ущерб информации в подразделении ОВД.

Среди основных типов событий присутствуют:

– нарушение порядка взаимодействия с Интернет-провайдерами, хостингами, почтовыми сервисами, облачными сервисами и другими поставщиками телекоммуникационных услуг;

– отказ оборудования по любым причинам, как технического, так и программного характера;

– нарушение работы программного обеспечения;

– нарушение любых правил обработки, хранения, передачи информации, как электронной, так и документов;

– неавторизированный или несанкционированный доступ третьих лиц к информационным ресурсам;

– выявление внешнего мониторинга ресурсов;

– выявление вирусов или других вредоносных программ;

– любая компрометация системы, например, попадание пароля от учетной записи в открытый доступ.

Все эти события должны быть классифицированы, описаны и внесены во внутренние документы компании, регламентирующие порядок обеспечения информационной безопасности. Кроме того, в регламентирующих документах необходимо установить иерархию событий, разделить их на более или менее значимые. Следует учитывать, что существенная часть инцидентов малозаметны, они происходят вне периметра внимания должностных лиц. Такие события должны быть описаны особо, и определены меры для их выявления в режиме постфактум.

При описании мер реакции следует учитывать, что изменение частоты появления и общего количества инцидентов информационной безопасности является одним из показателей качества работы систем, обеспечивающих ИБ, и само по себе классифицируется в качестве существенного события. Учащение событий может говорить о намеренной атаке на информационные системы компании, поэтому оно должно стать основанием для анализа и дальнейшего повышения уровня защиты.

1.2 Место управления инцидентами в общей системе информационной безопасности ИСОД МВД России

Регламенты, определяющие порядок управления инцидентами информационной безопасности, должны стать составной частью информационных процессов и их регламентации. Предполагая, что инцидентом является недозволенное, несанкционированное событие, в работе нужно опираться на механизм, разделяющий события и действия на

разрешенные и запрещенные, определяющий органы, имеющие права на разработку таких норм. Кроме того, регламент определяет методы и способы классификаций событий, прямо не обозначенных в документах в качестве значимых, и механизм выявления таких событий, их описания и последующего внесения в регламентирующие документы.

Например, в регламенте может быть запрещено размещение конфиденциальной информации на портативных носителях без ее кодировки или шифрования, при этом не будет прямо установлен запрет на вынос таких устройств за пределы компании. Случайная утрата компьютера в результате криминального посягательства станет инцидентом, но он не будет прямо запрещен. Соответственно, в документах должен быть установлен механизм дополнения норм и правил безопасности в ситуативном порядке без излишней бюрократии. Это позволит оперативно реагировать на новые вызовы и дорабатывать меры защиты своевременно, а не со значительным запозданием.

Система сертификации ISO 27001 в качестве одного из элементов информационной безопасности предполагает необходимость создания отдельной процедуры управления инцидентами информационной безопасности в рамках общей системы стандартизации информационных процессов.

Централизованный регламент обработки, передачи и хранения информации в телекоммуникационной системе МВД России на данный момент отсутствует, но, тем не менее, активно ведётся работа по обобщению существующих нормативных и организационных документов, которые позволят в ближайшем будущем иметь общий руководящий документ.

1.3 Особенности управления событиями безопасности в ИСОД МВД России

Несмотря на то, что стандарты прямо рекомендуют внедрять методики управления инцидентами информационной безопасности, на практике внедрение и реализация этих практик встречают множество сложностей. Отдельные процедуры управления инцидентами не внедряются. Этот показатель не говорит о том, что системы менеджмента инцидентов работают хорошо или плохо, это свидетельствует только о том, что существует определенная брешь в системе безопасности.

Управление инцидентами информационной безопасности в ИСОД МВД России должно быть основано на следующих действиях:

– определение. В организации отсутствует методика выявления и классификации инцидентов, описание их основных параметров, поэтому сотрудники встают перед необходимостью или самостоятельно определять критерии события, или игнорировать его. Вход в сеть под аккаунтом другого сотрудника, согласно стандартам, является инцидентом информационной безопасности, но он не будет зафиксирован в журнале, так как сотрудники считают такое поведение стандартным и дозволенным, особенно в условиях дефицита кадровых ресурсов;

– оповещение о возникновении. Даже если какое-либо событие может быть определено согласно принятым в организации методикам или личному мнению сотрудника как инцидент, чаще всего в организации не разработаны стандарты и маршруты оповещения о таких событиях. Даже если кем-то будет выявлен факт копирования документов, относящихся к коммерческой тайне, сотрудник встанет в тупик перед вопросом, кто именно и в какой форме должен быть оповещен об этом инциденте: его руководитель, служба безопасности или иное лицо;

– регистрация. Эта часть стандартов является наиболее невыполнимой для российских компаний, инциденты не идентифицируются, соответственно, не фиксируются. Отсутствует практика заведения регистров учета, в которых бы фиксировались значимые события, что впоследствии давало бы материал для их анализа и прогноза возможных атак;

– устранение причин и последствий. Любой инцидент вызывает определенные следы и последствия, которые, с одной стороны, могут мешать деятельности компании, с другой – служат материалом для проведения расследования причин его возникновения. Отсутствие регламентов устранения последствий может привести как к накоплению ошибок, так и к полному уничтожению доказательственной базы, позволяющей выявить виновника произошедшей ситуации. Любые срочные меры, предпринимаемые для восстановления стабильности, могут случайно или намеренно уничтожить следы проникновения в базу данных;

– меры реагирования на инциденты. В ряде случаев возникновение инцидента может потребовать срочных мер реагирования, например, отключения компьютера от сети, приостановки передачи информации, установки контакта с провайдером. Должны быть определены органы и должностные лица, ответственные за разработку механизма реагирования и его оперативную реализацию;

– расследование. Полномочия по расследованию должны быть переданы из ведения IT-службы в компетенцию служб безопасности. В рамках расследования должны быть изучены журналы учета, проанализированы действия всех пользователей и администраторов, которые имели доступ к системам в период возникновения чрезвычайной ситуации. Расследование должно стать одним из основных элементов управления инцидентами. На практике в российских компаниях от реализации этого этапа отказываются, ограничиваясь устранениями

последствий произошедшего события. При необходимости расследование должно производиться с привлечением оперативно-следственных органов;

– реализация превентивных мер. В большинстве случаев инциденты не являются единичными, их возникновение свидетельствует о том, что в системе ИБ возникла брешь и аналогичные случаи будут повторяться. Во избежание этих рисков необходимо по результатам расследования подготовить протокол или акт комиссии, в котором определить, какие именно меры должны быть применены для предотвращения аналогичных ситуаций. Кроме того, применяются определенные меры дисциплинарной ответственности, предусмотренные Трудовым кодексом и внутренними регламентами;

– аналитика. Все события, нарушающие регламентированные процессы и могущие быть квалифицированы в качестве инцидентов информационной безопасности, должны стать основой для анализа, который поможет определить их характер, проявить системность и выработать рекомендации для совершенствования системы ИБ, действующей в компании.

Основные проблемы, связанные с нарушением процедур, обусловлены неготовностью персонала в полной мере воспринимать, адаптировать и выполнять рекомендации. Касательно инцидентов информационной безопасности, сложности в восприятии и реакции вызывают моменты, связанные с совершением действий, которые прямо не регламентированы инструкциями или стандартами или вызывают ощущение излишних или избыточных.

1.4 Процедура управления инцидентами информационной безопасности

Как любая внутриведомственная процедура, организация управления инцидентами информационной безопасности в ИСОД МВД России должна пройти несколько этапов: от принятия решения о его необходимости до внедрения и аудита. На практике часто не осознаётся необходимость применения этих подходов защиты информационного периметра, поэтому для возникновения инициативы о ее внедрении часто требуется аудит систем информационной безопасности внешними консультантами, выработка ими рекомендаций, которые затем будут реализованы руководством предприятия. В случае с ИСОД МВД России такими консультантами выступает компания «IT-Consulting». Таким образом, начальной точкой для реализации процедур управления инцидентами информационной безопасности становится решение исполнительных органов.

Общее решение предлагается принимать в русле модернизации существующей системы информационной безопасности. Система управления инцидентами является ее основной частью. На уровне принятия решения необходима его локализация в общей парадигме целей МВД России. Оптимально, если функционирование системы информационной безопасности становится одной из целей Министерства, а качество ее работы подкрепляется установлением ключевых показателей эффективности для ответственных сотрудников. После определения статуса функционирования системы необходимо перейти к разработке внутренней документации.

Для придания значимости методикам управления информационной безопасностью они должны быть утверждены на уровне исполнительного органа (курирующего данное направление). С данными документа

необходимо ознакомить всех сотрудников, имеющих отношение к работе с информацией, существующей в электронных формах или на материальных носителях.

В структуре документа, оформляемого в виде положения или регламента, должны выделяться следующие подразделы:

– определение событий, признаваемых инцидентами применительно к системе безопасности конкретной компании. Так, пользование внешней электронной почтой может быть нарушением ИБ для государственной компании и рядовым событием для частной;

– порядок оповещения о событии. Должны быть определены формат уведомления (устный, докладная записка, электронное сообщение), перечень лиц, которые должны быть оповещены, и дублирующие их должности в случае их отсутствия, перечень лиц, до которых также доносится информация о событии (руководство компании), срок уведомления после получения информации об инциденте;

– перечень мероприятий по устранению последствий инцидента и порядок их реализации;

– порядок расследования, в котором определяются ответственные за него должностные лица, механизм сбора и фиксации доказательств, возможные действия по выявлению виновника;

– порядок привлечения виновных лиц к дисциплинарной ответственности;

– меры усиления безопасности, которые должны быть применены по итогам расследования инцидента;

– порядок минимизации вреда и устранения последствий инцидентов.

При разработке регламентов, опосредующих систему управления событиями информационной безопасности, желательно опираться на уже созданные и показавшие свою эффективность методики и документы, включая формы отчетов, журналы регистрации, уведомления о событии.

1.5 Установление причин и анализ последствий реализации инцидента информационной безопасности

Непосредственно после уведомления соответствующих должностных лиц о произошедшем инциденте и его фиксации необходимо совершить действия реагирования, а именно устранения причин и последствий события. Все этапы этих процессов должны найти свое отражение в регламентах. Там описываются перечни общих действий для отдельных наиболее значимых событий, конкретные шаги и сроки применения мер. Необходимо также предусмотреть ответственность за неприменение установленных мер или недостаточно эффективное их применение.

На этапе расследования от должностных лиц организации требуется:

– определить причины возникновения инцидента и недостатки регламентирующих документов и методик, сделавших возможным его возникновение;

– установить ответственных и виновных лиц;

– собрать и зафиксировать доказательства;

– установить мотивы совершения инцидента и круг лиц, причастных к нему помимо сотрудников, выявить заказчика.

Если предполагается в дальнейшем возбуждение судебного преследования по факту инцидента на основании совершения преступления в сфере информационной безопасности или нарушения конфиденциальности служебной информации, к расследованию уже на начальном этапе необходимо привлечь оперативно-следственные органы. Собранные самостоятельно факты без соблюдения процессуальных мер не будут признаны надлежащими доказательствами и приобщены к делу.

Непосредственно после выявления инцидента предпринимаются оперативные меры по устранению его последствий. На следующем этапе

необходим анализ причин его возникновения и совершение комплекса действий, направленных на предотвращение возможного повторения аналогичного события. Сегодня основным регламентирующим документом, предлагающим стандарты реакции на инциденты, стал ISO/IEC 27000:2016, это последняя версия совместной разработки ISO и Энергетической комиссии. В России на основе более ранних версий ISO/IEC разработаны ГОСТы. В рамках ISO/IEC 27000:2016 предлагается создать специальную службу поддержки, на которую должны быть возложены функции управления инцидентами.

1.6 Аудит соблюдения регламента безопасности

При получении сертификата соответствия по стандарту ISO 27001, а также при проверке соблюдений требований стандарта проводится аудит выполнения методик управления инцидентами информационной безопасности. При проведении аудита часто выясняется, что даже при внедрении стандартов возникает существенное количество проблем, связанных с регистрацией инцидентов и расследованием событий, послуживших причиной для их возникновения. Расследования осложняются тем, что под одной учетной записью могут входить несколько операторов или администраторов, что затрудняет их аутентификацию. На контроллере серверов в ИСОД МВД России в большинстве случаев не заводятся и не ведутся журналы учета событий. Отсутствие контролируемой системы идентификации пользователей, характерное для большинства российских компаний, позволяет в произвольном режиме менять информацию, останавливать серверы или модифицировать их работу.

Рекомендуется проведение аудита не реже чем раз в полгода. Его результатами должны стать обновление перечня событий, признаваемых

инцидентами, доработка перечня необходимых действий по их устранению, изменение программных средств, обеспечивающих защиту информационного периметра. Если в телекоммуникационной системе МВД России будут планироваться к интеграции DLP-системы и SIEM-системы, то с учетом проведенного анализа инцидентов, произошедших за определенный период, и результатов аудита они могут быть доработаны.

Аудит не должен быть единственным фактором, выявляющим недостатки работы системы. Еще на этапе ее внедрения должны быть разработаны системы контроля качества процессов, результаты работы которых должны обрабатываться в регулярном режиме.

2. Система предупреждения и обнаружения инцидентов информационной безопасности в компьютерных сетях «Форпост»

2.1. Общие сведения о системе

Система обнаружения компьютерных атак (СОА) «Форпост» версии 2.0, РМАГ.00026-20, предназначена для автоматического выявления воздействий на контролируемую данным средством автоматизированную информационную систему (АИС), которые могут быть классифицированы как компьютерные атаки.

СОА «Форпост» обеспечивает:

− обнаружение компьютерных атак, направленных на сервера телематических служб (WEB, FTP, электронная почта, СУБД и пр.) и рабочие станции, размещенные в контролируемых сегментах АИС;

− предотвращение развития сетевых компьютерных атак путем блокирования источников атак посредством отправки сетевому оборудованию (межсетевому экрану, коммутатору, маршрутизатору), по протоколам RS-232, telnet, соответствующей последовательности команд на основе шаблонов;

− оповещение администратора безопасности об обнаруженных атаках путем вывода соответствующего сообщения на консоль администратора СОА, записи сообщения в специальный журнал, путем отправки сообщений по электронной почте;

− контроль целостности собственных ресурсов СОА и ресурсов защищаемой АИС, а так же, за счет этого механизма, возможность отслеживания действий нарушителей по отношению к контролируемым ресурсам в скомпрометированной системе;

− оповещение администратора безопасности о новых сообщениях системных журналов на машинах защищаемой АИС путем вывода

соответствующего сообщения на консоль администратора СОА, записи сообщения в специальный журнал, путем отправки сообщений по электронной почте;

− ведение журнала системных сообщений, содержащего служебную информацию, формируемую компонентами СОА, журнала сообщений от сетевого оборудования, поступающих по протоколам SNMP и syslog;

− удаленное управление сетевым оборудованием по защищенному с использованием отечественных средств криптографической защиты информации (СКЗИ) каналу;

− интеграцию с внешними системами путем передачи сообщений о зафиксированных компьютерных атаках из журнала СОА по протоколу syslog;

− генерацию отчетов на основе содержимого журналов СОА.

Продукт обладает подсистемой собственной безопасности, которая позволяет шифровать передаваемую между компонентами информацию с использованием отечественных СКЗИ, осуществлять контроль целостности собственных ресурсов и ресурсов защищаемой АИС.

2.2. Основные характеристики системы

В основу функционирования сетевого датчика СОА «Форпост» положен сигнатурный метод выявления атак. Он обеспечивает обнаружение атак на основе специальных шаблонов (сигнатур), каждый из которых соответствует конкретной атаке. При получении исходных данных о сетевом трафике информационной системы, СОА «Форпост» производит их анализ на соответствие указанным шаблонам атак, имеющихся в базе данных. В случае обнаружения сигнатуры в исходных данных, система регистрирует факт обнаружения атаки, оповещает администратора безопасности о данном событии и предоставляет

возможность администратору произвести блокирование источника атаки с помощью соответствующего коммуникационного оборудования.

За счет использования датчиков контроля целостности СОА позволяет отслеживать действия нарушителя по отношению к контролируемым ресурсам в скомпрометированной системе.

Дополнительно поддерживается получение данных о функционировании отдельных объектов контролируемой АИС по протоколам syslog и SNMP.

СОА «Форпост» реализует следующие методы реагирования на факт выявления компьютерной атаки:

− идентификация компьютерной атаки с использованием описаний уязвимостей, на которые они направлены, или описаний реализаций компьютерных атак;

− оповещение администратора безопасности об обнаруженных атаках путем вывода соответствующего сообщения на консоль администратора СОА, отправки сообщений по электронной почте;

− регистрация атаки в журнале модулей-датчиков СОА;

− блокировка источника угрозы информационной безопасности путем блокирования источников атак посредством отправки сетевому оборудованию (межсетевому экрану, коммутатору, маршрутизатору), по протоколам RS-232, telnet, последовательности команд на основе шаблонов.

Управление сетевым оборудованием производится компонентом СОА через локальный интерфейс RS-232 или через выделенный сетевой интерфейс с использованием протокола telnet. Связь между удаленной консолью администратора и компонентом СОА, выполняющим управление сетевым оборудованием осуществляется по защищенному с использованием отечественных СКЗИ каналу.

СОА «Форпост» обеспечивает возможность выборочного контроля ресурсов защищаемой АИС, контроль целостности собственных ресурсов (исполняемых и конфигурационных файлов, веток реестра) СОА и ресурсов защищаемой АИС. Также СОА «Форпост» позволяет получать новые сообщения системных журналов контролируемой АИС.

СОА «Форпост» выявляет компьютерные атаки на основе анализа сетевого трафика контролируемой АИС на сетевом, транспортном и прикладном уровнях стека протоколов TCP/IP.

СОА «Форпост» имеет консоль администратора, которая реализует механизм удаленного управления данным средством. Дополнительно система имеет механизм локального управления, позволяющий: производить настройку своих компонентов, их запуск, остановку и перезапуск; формировать, редактировать и подписывать электронной цифровой подписью администратора СОА список контролируемых на целостность ресурсов.

С целью маскирования СОА «Форпост» в составе контролируемой АИС предполагается выделение СОА в отдельный сегмент, если на защищаемых объектах не установлены датчики контроля целостности, или отделение компонентов СОА от возможных нарушителей с помощью межсетевых экранов, исключая точки съема информации сетевыми датчиками.

В качестве дополнительной меры по затруднению демаскирования компонентов СОА предусмотрена возможность наложения ограничений на сетевые адреса, между которыми осуществляется взаимодействие компонентов.

СОА «Форпост» реализует следующие механизмы собственной защиты:

− обеспечивается идентификацию и аутентификацию администратора СОА при запуске

консоли администратора по имени пользователя и паролю; ведется контроль длины создаваемых паролей (не менее 6 символов) и состав паролей (буквенно-цифровые);

− в процессе работы осуществляется контроль целостности компонентов и конфигураций СОА;

− СОА имеет функцию сигнализации администратору СОА о неверных попытках аутентификации при доступе к консоли администратора, в частности, сигнализации о трех подряд неверных попытках аутентификации путем записи соответствующего события в системный журнал и отсылки сообщения электронной почты;

− управляющая информация, служебная информация компонентов и данные о выявленных компьютерных атаках могут передаваться между компонентами в зашифрованном виде с использованием СКЗИ КриптоПро 3.6 по протоколу TLS;

− предусмотрена возможность наложения ограничений на адреса, с которых осуществляется удаленное администрирование СОА.

СОА «Форпост» имеет автоматизированный механизм обновления базы решающих правил, позволяющий загружать сигнатуры компьютерных атак на датчики, с использованием консоли администратора.

Дополнительно имеются штатные средства задания новых сигнатур компьютерных атак с использованием языка описания сигнатур.

СОА «Форпост» регистрирует в своих журналах:

− сведения о выявленных компьютерных атаках и случаях нарушения целостности контролируемых ресурсов;

− сведения о сообщениях системных журналов с машин контролируемых ресурсов.

− служебную информацию, формируемую компонентами СОА, такую как подключение или отключение компонентов СОА, вход и выход

администратора СОА в консоль администратора, информацию о блокировке или разблокировке источника атаки и пр.

− сообщения от сетевого оборудования, поступающие по протоколам SNMP и syslog.

СОА «Форпост» имеет функцию периодического создания резервных копий базы данных СОА в отдельный файл с последующим выводом соответствующего сообщения на консоль администратора СОА.

Дополнительные характеристики СОА «Форпост»:

− может применяться в АИС с производительностью до 1 ГБита/с;

− имеет механизм фильтрации событий, отображаемых в журналах СОА;

− обладает интуитивно-понятным русскоязычным графическим интерфейсом администрирования;

− работает под управлением операционных систем Windows XP/7, Windows Server 2003/2008;

− поддерживает интеграцию с внешними системами (например, с различными системами корреляции: Cisco Mars, ArcSight и др.) путем отсылки сообщений о компьютерных атаках из журнала СОА по протоколу syslog;

− имеет возможность генерации табличных и текстовых отчетов на основе содержимого журналов СОА;

− имеет распределенную модульную архитектуру, обеспечивающую масштабируемость системы, позволяющую адаптироваться под требования конкретной АИС по производительности и отказоустойчивости: в зависимости от используемых аппаратных мощностей и настроек СОА может использоваться для мониторинга каналов со скоростью до 1 Гбита/с; существует возможность резервирования ключевых компонентов.

2.3. Логическая структура системы

СОА «Форпост» имеет распределенную многомодульную архитектуру. Модули могут быть установлены как на один сервер, так и распределены на несколько в зависимости от требуемых показателей производительности и отказоустойчивости.

Информационный фонд представляет собой базу данных, работающую под управлением СУБД MS SQL 2005/2008, специальный компонент «Агент БД», и обеспечивает:

− централизованное хранение событий системы;

− централизованное хранение шаблонов датчиков и базы сигнатур СОА.

Компонент «Агент БД» в связке с **CryptoODBC-драйвером** из состава СОА «Форпост» обеспечивает криптографически защищенный с использованием отечественных СКЗИ информационный обмен между информационным фондом и компонентами СОА, которые к нему подключаются (координационный центр, модуль почтовых уведомлений).

Координационный центр является связующим звеном между модулями системы:

обеспечивает передачу информации между ними, выполняет функции контроля работоспособности компонентов.

Консоль администратора обеспечивает графический пользовательский интерфейс

системы, посредством которого обеспечивается управление и мониторинг состояния СОА.

Модуль интеграции с сетевым оборудованием предназначен для:

− установления и поддержания подключения к сетевому оборудованию (межсетевые экраны, коммутаторы, маршрутизаторы) по протоколам RS-232, telnet;

− управления сетевым оборудованием (блокировка источников угроз на основе ранее написанных шаблонов, ручное управление);

− получения системных сообщений от сетевого оборудования (по протоколам SNMP и syslog);

− интеграции с внешними системами (например, с различными системами корреляции: Cisco Mars, ArcSight и др.) путем отсылки сообщений о компьютерных атаках из журнала СОА по протоколу syslog.

Модуль почтовых уведомлений позволяет автоматически по электронной почте отправлять заранее заданным адресатам информацию об обнаруженных атаках и событиях, происходящих в системе.

Агент выполняет функции управления датчиками, а также функции обеспечения передачи информации между датчиками и координационным центром. К одному агенту может быть подключен один датчик контроля целостности и несколько сетевых датчиков.

Сетевой датчик осуществляет анализ поступающего трафика на наличие в нем компьютерных атак используя сигнатурный метод; подключается к зеркалирующему (SPAN) порту коммутатора, межсетевого экрана, специализированного ответвителя трафика (TAP) и пр.

Датчик контроля целостности производит контроль целостности собственных ресурсов (исполняемых и конфигурационных файлов, веток реестра) СОА и ресурсов защищаемой АИС. Также датчик контроля целостности позволяет получать новые сообщения системных журналов.

СОА «Форпост» предъявляет следующие минимальные системные требования:

− операционная система для информационного фонда, координационного центра и сетевого датчика – Windows Server 2003/2008, для остальных компонентов – Windows XP/7, Windows Server 2003/2008;

− процессор с частотой не менее 1,6 ГГц;

− оперативной памяти не менее 1024 МБ;

− объем свободного дискового пространства не менее 20 ГБ;

− сетевой интерфейс со скоростью не менее 100 Мбит/с;

− на сервере с сетевым датчиком – дополнительно не менее 1 сетевого интерфейса для захвата трафика со скоростью не менее 100 Мбит/с предпочтительно в серверном исполнении.

Поскольку система распределенная, компоненты СОА могут быть установлены как на один сервер, так и распределены на несколько физических серверов.

При повышенных требованиях по производительности рекомендуется:

− на серверах с информационным фондом, координационными центрами, сетевыми датчиками увеличить тактовую частоту процессора и использовать многоядерные, либо многопроцессорные конфигурации; использовать серверные версии операционной системы Windows;

− на серверах с сетевыми датчиками увеличить объем оперативной памяти до 2-4 ГБ;

− привести объем дискового пространства в соответствие с потребностями информационного фонда по объему единовременно хранимой в системе информации о событиях;

− на серверах с сетевыми датчиками для захвата трафика использовать сетевые интерфейсы со скоростью 1 Гбит/с в серверном исполнении.

Дополнительные сведения о выборе аппаратной конфигурации для компонентов СОА «Форпост» в зависимости от требований по производительности приведены в документе «Описание применения», РМАГ.00026-20 31 01.

Для того, что бы сетевой датчик мог обрабатывать поток трафика со скоростью 1 Гбит/с, число процессорных ядер должно быть не менее 8 шт.

Для обработки трафика со скоростью 500 Мбит/с, число процессорных ядер должно быть не менее 4 шт. При использовании нескольких сетевых датчиков на одном физическом сервере технология Hyper-Threading должна быть отключена.

Дополнительные сведения о производительности сетевого датчика и возможных вариантах его конфигурации приведены в п. 4.8 данного документа и в документе «Описание применения», РМАГ.00026-20 31 01.

2.4 Особенности применения системы

СОА «Форпост» имеет следующие особенности применения:

− необходимо своевременно проводить техническое обслуживание системы в соответствии с регламентом, описанном в руководстве администратора, РМАГ.00026-20 90 01;

− уведомление администратора о возникновении ситуации, требующей его внимания, возможно через консоль администратора, всплывающее окно, по электронной почте;

− хранение всей накопленной системой информации о процессах в АИС на протяжении достаточно длительных периодов может приводить к уменьшению производительности, что связано с большими объемами данных, обрабатываемых системой, поэтому в ходе эксплуатации СОА «Форпост» необходимо производить периодическое резервное копирование и удаление несущественной информации (одновременно консоль администратора в журнале модулей-датчиков может выводить на экран не более 100 000 записей);

− размер буфера у агентов, в котором они накапливают информацию, полученную от датчиков и подлежащую отправке в координационный центр, фиксированный и информация в нем обновляется циклически (старые события, подлежащие отправке в координационный центр по

достижению максимального размера буфера затираются более новыми), что в случае недостаточной пропускной способности канала связи (или каких-либо других факторов) может приводить к потере части данных;

− приложением поддерживается работа с протоколом IP версии 4, протокол IP версии 6 – не поддерживается.

СОА «Форпост» предъявляет высокие требования к квалификации и компетентности эксплуатирующего персонала, связанные со спецификой предметной области.

2.5 Специфика развёртывания системы

Для установки компонентов СОА «Форпост» пользователь должен обладать правами администратора.

Поскольку система является распределенной, компоненты могут устанавливаться как на отдельные выделенные машины, так и совмещаться друг с другом в рамках одной или нескольких выделенных машин. Операционная система, необходимая для работы информационного фонда, координационного центра и сетевого датчика – Windows Server 2003/2008, для остальных компонентов – Windows XP/7, Windows Server 2003/2008.

Перед установкой СОА «Форпост» необходимо провести установку следующего программного обеспечения:

1) криптопровайдер КриптоПро CSP (если требуется шифрование информационного обмена между компонентами СОА, контроль целостности ресурсов с использованием отечественных криптоалгоритмов) – на каждом узле, на котором будут устанавливаться компоненты СОА;

2) СУБД Microsoft SQL Server (под управлением которой работает информационный фонд) – на сервере информационного фонда.

В общем случае компоненты СОА «Форпост» устанавливаются в следующей последовательности:

1) информационный фонд;

2) координационный центр (основной и, при необходимости, резервный) и, опционально, модуль почтовых уведомлений;

3) консоль администратора;

4) агенты;

5) датчики (сетевой, контроля целостности).

Функциональность модуля интеграции с сетевым оборудованием интегрирована в агент и координационный центр. Таким образом, существует возможность управлять сетевым оборудованием, подключенным локально к узлам, на которые установлены указанные выше модули СОА.

Модуль почтовых уведомлений устанавливается на тот же самый узел, на который устанавливается координационный центр.

Агенты устанавливаются на все узлы, на которых должны функционировать датчики СОА.

По умолчанию предполагается, что связь координационных центров с СУБД, установленной на сервере информационного фонда, будет осуществляться с использованием ODBCдрайвера из состава СОА «Форпост». Для корректной работы этого драйвера при установке информационного фонда необходимо не отказываться от установки компонента «Агент БД». Использование ODBC-драйвера из состава СОА «Форпост» вместо драйвера из комплекта поставки операционной системы или СУБД является обязательным, если предполагается шифрование информационного обмена между координационными центрами и информационным фондом с использованием отечественных криптоалгоритмов.

Для удобства консоль администратора, координационный центр и модуль почтовых уведомлений объединены в один установочный пакет.

Информационный фонд и агент выделены в отдельные установочные пакеты.

Информационный фонд, координационный центр и консоль администратора и модуль почтовых уведомлений должны устанавливаться локально.

Агент может быть установлен как локально, так и удаленно. Выбор метода установки зависит от специфики автоматизированной информационной системы (АИС), в которую производится встраивание СОА: следует учитывать, что удаленная установка агента производится через стандартный административный общий ресурс ADMIN$ по протоколу NetBIOS, при этом данные передаются в незашифрованном виде. Если на момент разворачивания СОА шифрование передаваемых между компонентами СОА данных является обязательным, то следует выбирать локальную установку агента.

Установка датчиков производится удаленно с консоли администратора СОА.

Пользователи, не обладающие правами настройки СОА «Форпост» не должны иметь доступа на запись в каталог, в который производилась установка СОА.

2.6 Особенности настройки межсетевых экранов защищаемого сегмента ИСОД МВД России

Сведения из данного раздела могут использоваться для настройки как аппаратных межсетевых экранов, если их использование предусмотрено схемой включения, так и различных программных межсетевых экранов, установленных на узлы, на которых будут работать компоненты СОА «Форпост», в том числе межсетевой экран, входящий в поставку ОС семейства Windows.

Если на узлах, на которых установлены компоненты СОА «Форпост», либо между узлами с установленными компонентами СОА «Форпост», установлен межсетевой экран, для корректной работы компонентов СОА «Форпост» необходимо провести его настройку.

По умолчанию координационный центр ожидает подключение на порт 10000/TCP, если шифрование информационного обмена между компонентами СОА не используется; и на порт 10001/TCP, если используется шифрование информационного обмена; информационный фонд ожидает подключение на порт 10002/TCP, если шифрование информационного обмена между компонентами СОА не используется; и на порт 10003/TCP, если используется шифрование информационного обмена.

Настройка межсетевого экрана производится в соответствии со следующими положениями:

1) необходимо разрешить узлам с установленными компонентами агент и консоль администратора доступ к узлу (-ам) с установленным координационным центром (основным и резервным);

2) узлу (-ам) с установленным координационным центром (основным и резервным) необходимо разрешить доступ к серверу информационного фонда;

3) узлу, с установленным модулем почтовых уведомлений необходимо разрешить доступ к серверу информационного фонда и SMTP-серверу, на который осуществляется отправка почтовых уведомлений (порт 25/TCP);

4) если предполагается удаленная установка (удаление) агента, то необходимо разрешить протокол NetBIOS между координационным центром (-ами) и узлами, на которые предполагается устанавливать (удалять) агент;

5) если предполагается использование возможностей модуля интеграции с сетевым оборудованием в части приема SNMP-сообщений, приема/отправки syslog-сообщений, либо управления сетевым оборудованием по протоколу telnet, то на межсетевом экране необходимо разрешить использование данных протоколов (по умолчанию для протокола SNMP: 162/UPD, для протокола syslog: 514/UDP, для проткола telnet: 23/TCP);

6) при необходимости, если предполагается использование криптографически защищаенного (шифрованного) информационного обмена между компонентами СОА или использование функции контроля целостности ресурсов, необходимо разрешить узлам с установленными компонентами СОА «Форпост» доступ к web-серверу, на котором публикуется список отозванных сертификатов.

Использование конкретных прикладных протоколов, перечисленных выше, при работе с СОА «Форпост», и возможность их разрешить на аппаратном межсетевом экране, предусмотренном типовой схемой включения СОА «Форпост» в автоматизированную информационную систему (рисунок 2.2 документа «Описание применения», РМАГ.00026-20 31 01) определяется требованиями конкретной АИС.

2.7 Особенности установки внешнего криптопровайдера КриптоПро CSP

В случае, если требуется шифрование информационного обмена между компонентами СОА «Форпост», контроль целостности ресурсов с использованием отечественных криптоалгоритмов, на узлы, на которых будут устанавливаться компоненты СОА необходимо установить внешний криптопровайдер. Данная версия СОА «Форпост» проверялась на совместимость с криптопровайдером КриптоПро CSP 3.6.

Установка криптопровайдера осуществляется на каждом узле, на котором будут устанавливаться компоненты СОА.

На узлы, на которых установлены компоненты СОА «Форпост» координационный центр и информационный фонд – требуется серверная лицензия на КриптоПРО CSP. Для узлов, на которых не установлены вышеперечисленные компоненты, достаточно иметь клиентскую лицензию на КриптоПРО CSP.

Криптопровайдер устанавливается и настраивается в соответствие с эксплуатационной документацией на него и требованиями конкретной АИС, в которую производится встраивание СОА.

2.8 Специфика установки информационного фонда

Информационный фонд СОА «Форпост» работает под управлением СУБД Microsoft SQL Server 2005/2008. Допускается использование SQL Server 2005/2008 Express Edition.

Для сетевого адаптера сервера с информационным фондом должен быть определен статический IP-адрес.

По умолчанию предполагается, что связь координационных центров с СУБД информационного фонда будет осуществляться с использованием ODBC-драйвера из состава СОА «Форпост». Для корректной работы этого драйвера при установке информационного фонда необходимо не отказываться от установки компонента «Агент БД». Использование ODBC-драйвера из состава СОА «Форпост» вместо драйвера из комплекта поставки операционной системы или СУБД является обязательным, если предполагается шифрование информационного обмена между координационным центрами и информационным фондом с использованием отечественных криптоалгоритмов.

Допускается использование ODBC-драйвера из комплекта поставки операционной системы или СУБД в случае, если информационный фонд и координационный центр предполагается устанавливать на одном сервере, а так же в случае, если шифрование информационного обмена между координационными центрами и информационным фондом с использованием отечественных криптоалгоритмов не требуется.

До установки информационного фонда необходимо произвести установку СУБД MS SQL Server, учитывая следующие особенности:

− необходимо выбрать смешанный режим проверки подлинности;

− если информационный фонд и координационный центр (с модулем почтовых уведомлений) устанавливаются на разных узлах и по каким-то причинам предполагается отказаться от использования ODBC-драйвера из состава СОА «Форпост», в настройках СУБД следует разрешить удаленные соединения через локальную сеть (в версии Express Edition СУБД MS SQL Server по умолчанию данные соединения запрещены);

− при установке СУБД при выборе компонентов для работы СОА «Форпост» и возможности восстановления ее после сбоев обязательно необходимо установить «Службы компонента Database Engine» и «Средства управления – полный набор».

Ниже приводится типовая инструкция по установке СУБД MS SQL Server 2008.

2.9 Установка СУБД MS SQL Server

Для установки необходимо запустить файл «setup.exe», расположенный в корне дистрибутива с Microsoft SQL Server 2008.

При необходимости программа установки запустит установку Microsoft .NET Framework (рисунок 2.1) и необходимых обновлений операционной системы. Нажмите кнопку «ОК».

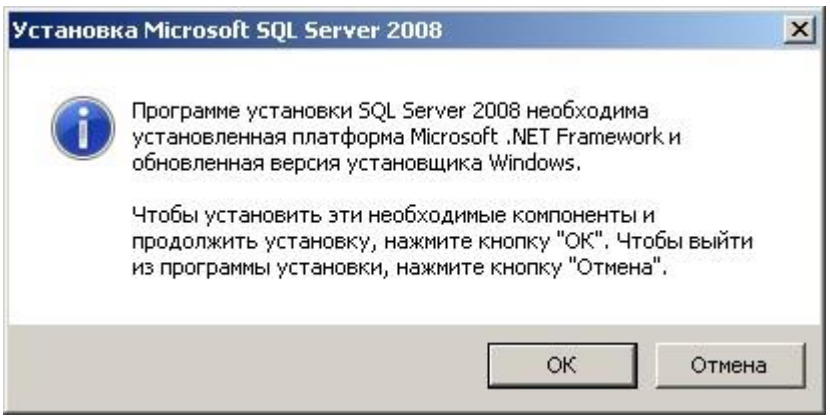

Рисунок 2.1

В следующем окне (рисунок 2.2) необходимо прочитать лицензионное соглашение, отметить пункт «Я прочитал(а) и ПРИНИМАЮ условия лицензионного соглашения» и нажать кнопку «Установить».

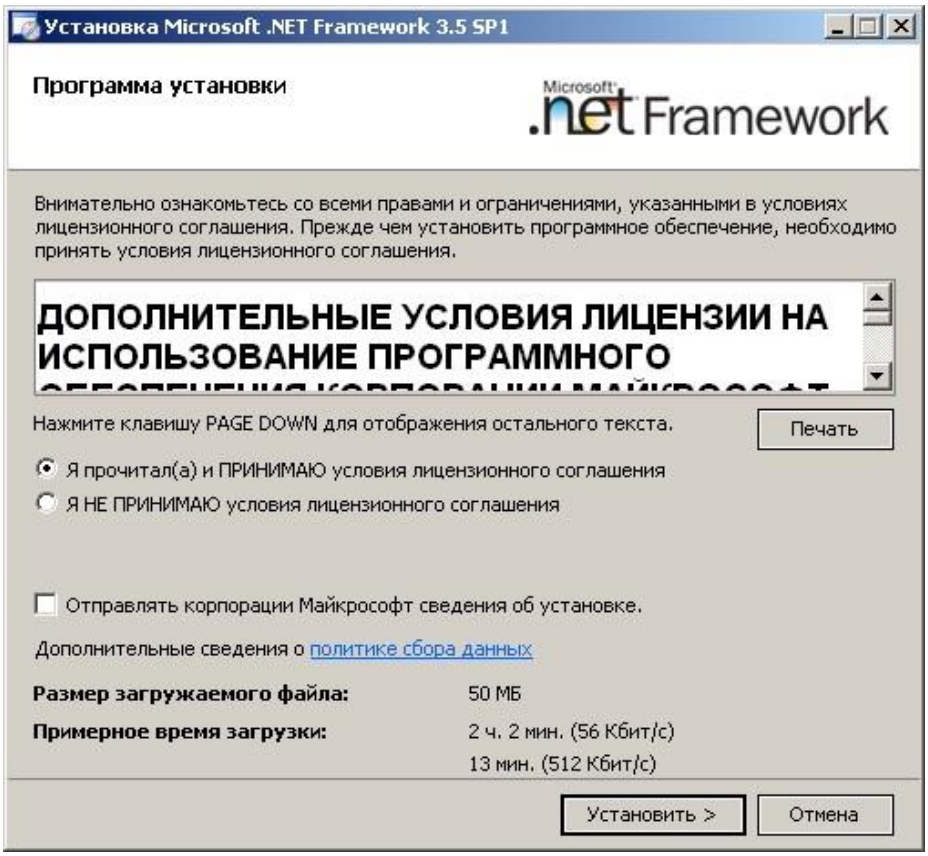

Рисунок 2.2

Дождитесь окончания установки (рисунок 2.3). По окончании установки нажмите кнопку «Выход» (рисунок 2.4).

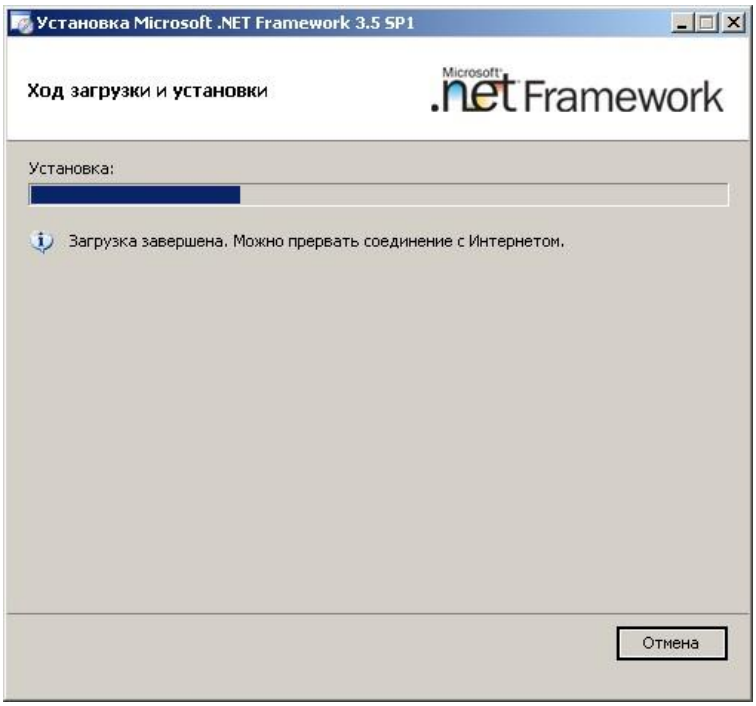

Рисунок 2.3

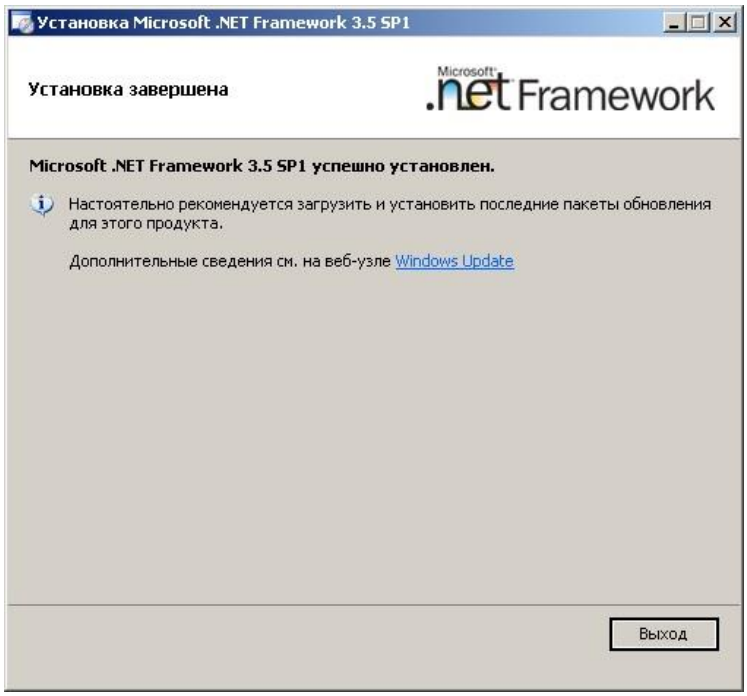

Рисунок 2.4

Далее при необходимости будет предложена установка необходимых обновлений на операционную систему (рисунок 2.5). Необходимо провести их установку. Нажмите кнопку «ОК».

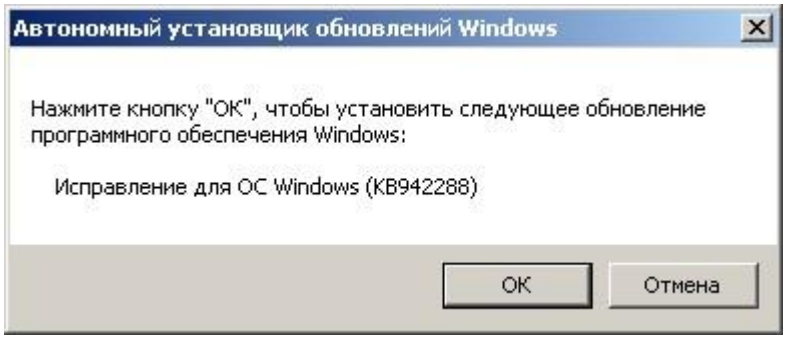

Рисунок 2.5

Дождитесь окончания установки (рисунок 2.6).

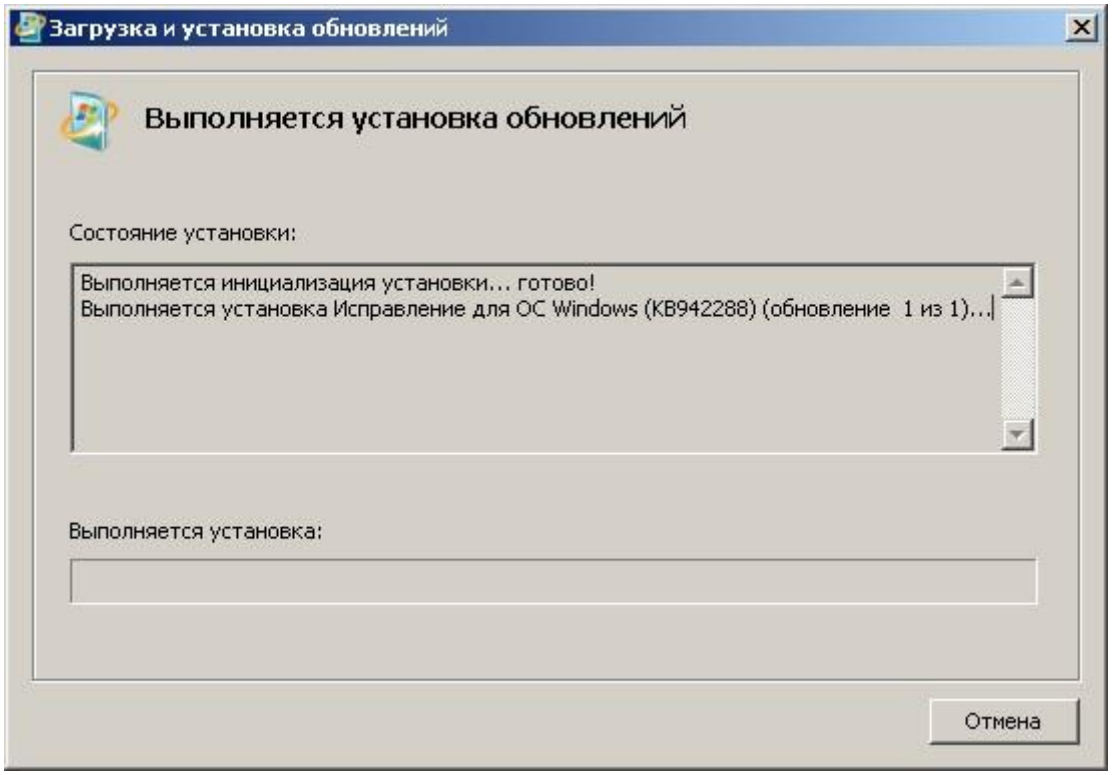

Рисунок 2.6

По окончании установки обновлений и дополнительных обязательных компонентов будет предложено перезагрузить компьютер (рисунок 2.7). Нажмите кнопку «Перезагрузить сейчас».

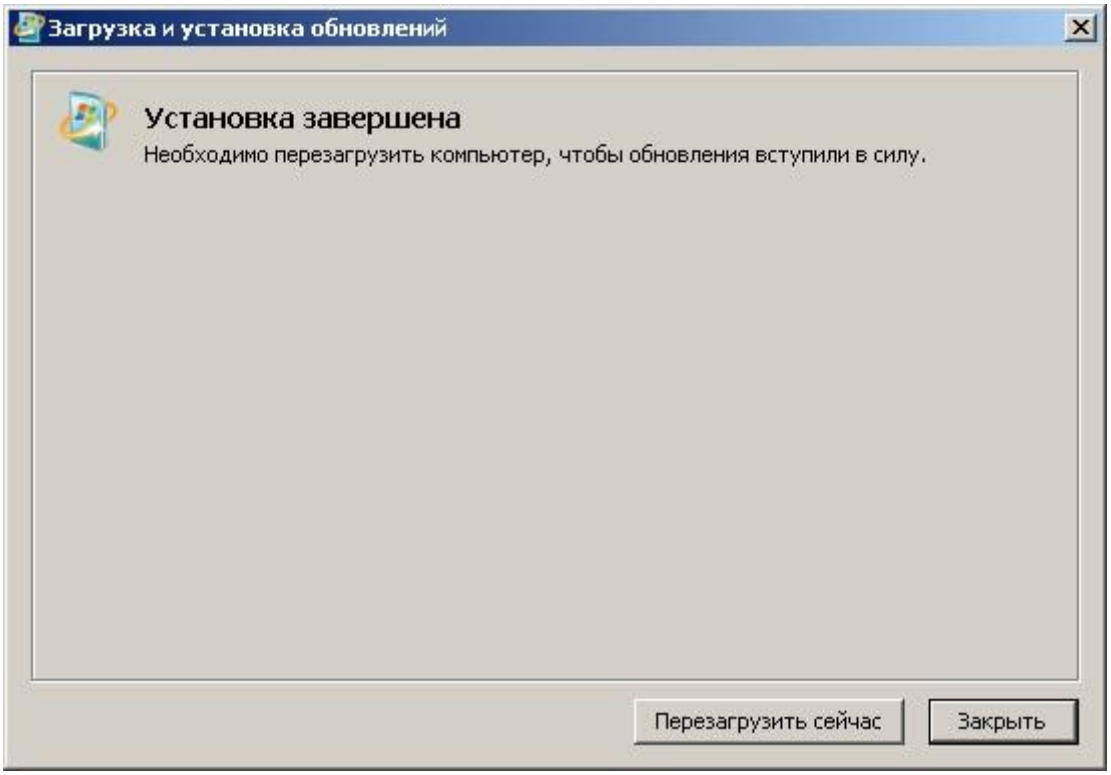

Рисунок 2.7

Далее необходимо запустить файл «setup.exe», расположенный в корне дистрибутива с Microsoft SQL Server 2008. Появится меню (рисунок 2.8), в котором с левой стороны необходимо выбрать пункт «Установка». Далее необходимо выбрать пункт «Новая установка изолированного SQL Server или добавление компонентов к существующему экземпляру».

В появившемся окне (рисунок 2.9) необходимо нажать кнопку «ОК».

В следующем окне (рисунок 2.10) необходимо нажать кнопку «Далее» (при необходимости предварительно введя ключ продукта).

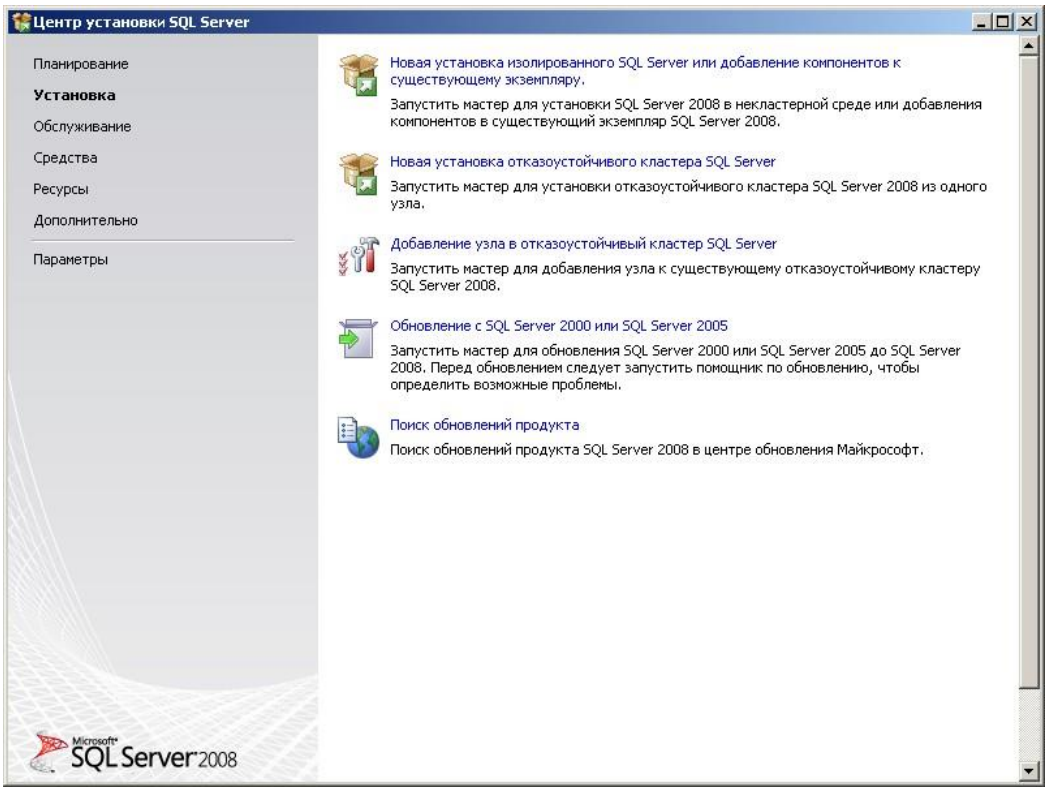

Рисунок 2.8

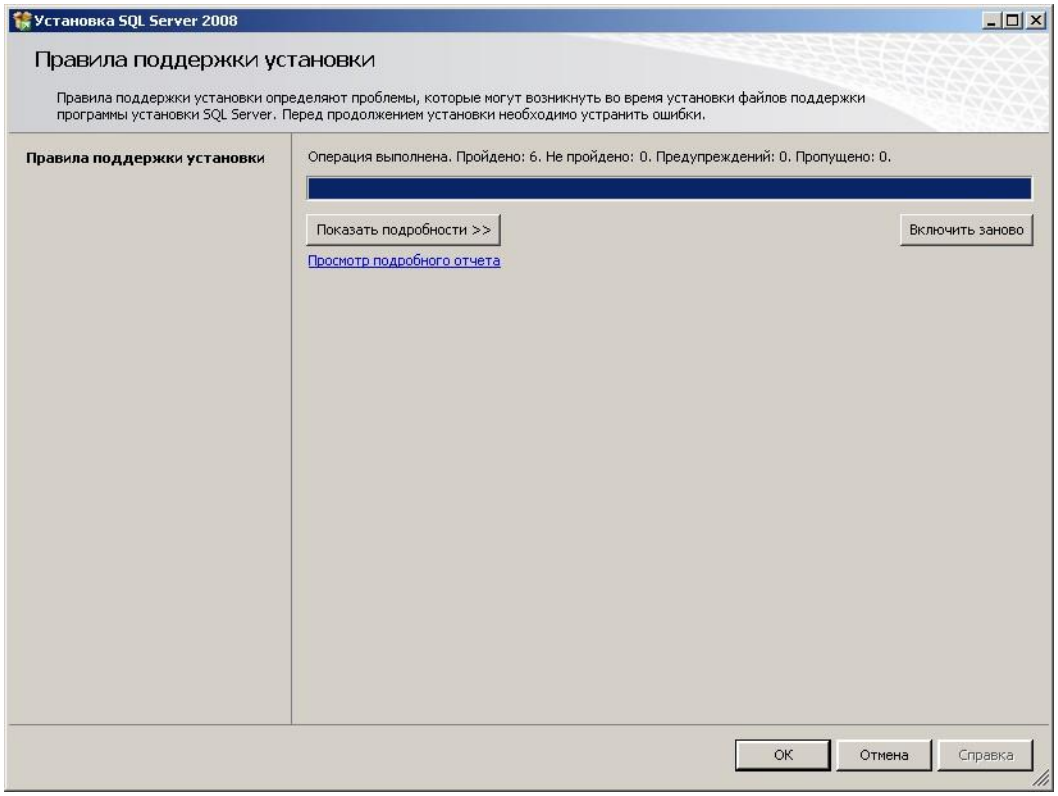

Рисунок 2.9

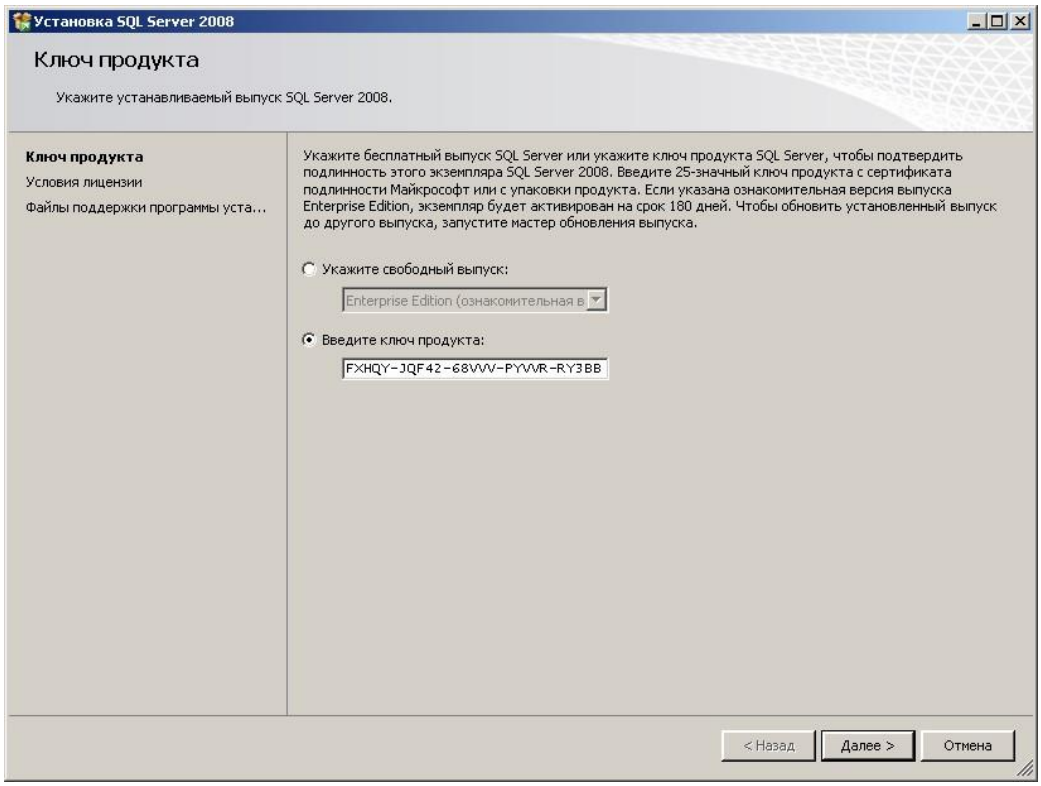

Рисунок 2.10

В следующем окне (рисунок 2.11) необходимо ознакомиться с условиями лицензии, отметить пункт «Я принимаю условия лицензионного соглашения» и нажать кнопку «Далее >». В следующем окне (рисунок 2.12) необходимо нажать кнопку «Установить».

В следующем окне (рисунок 2.13) необходимо нажать кнопку «Далее >».

В следующем окне (рисунок 2.14) необходимо выбрать следующие компоненты: «Службы компонента Database Engine», «Средства управления – основные», «Средства управления – полный набор» и нажать кнопку «Далее >».

В следующем окне (рисунок 2.15) необходимо выбрать параметр «Экземпляр по умолчанию», указать путь установки и нажать кнопку «Далее >».

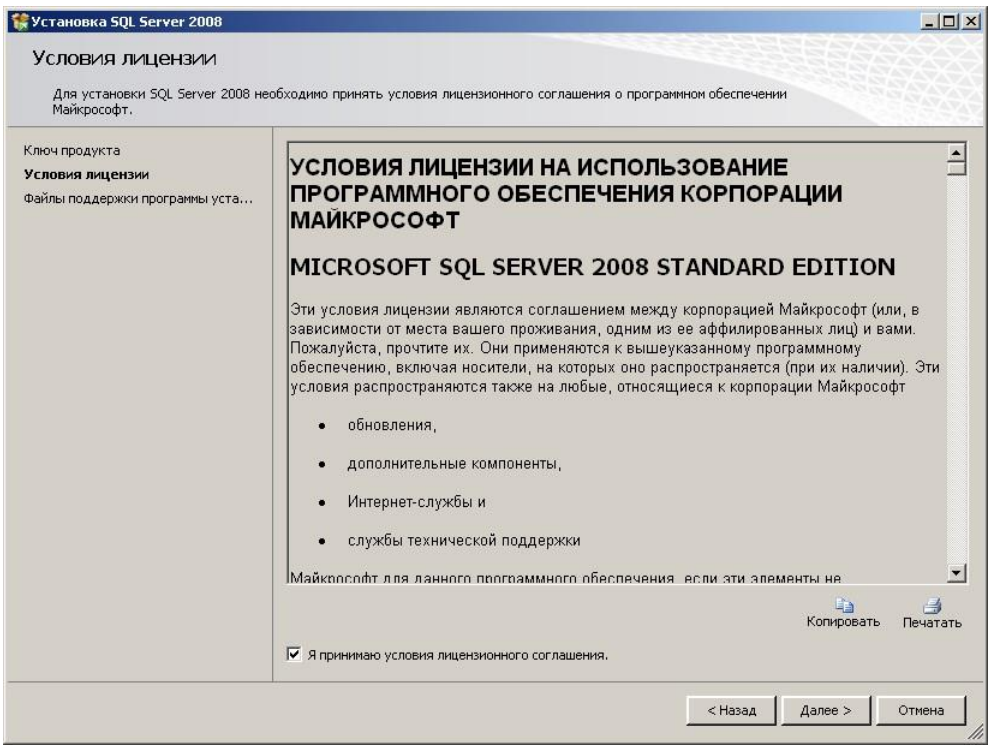

Рисунок 2.11

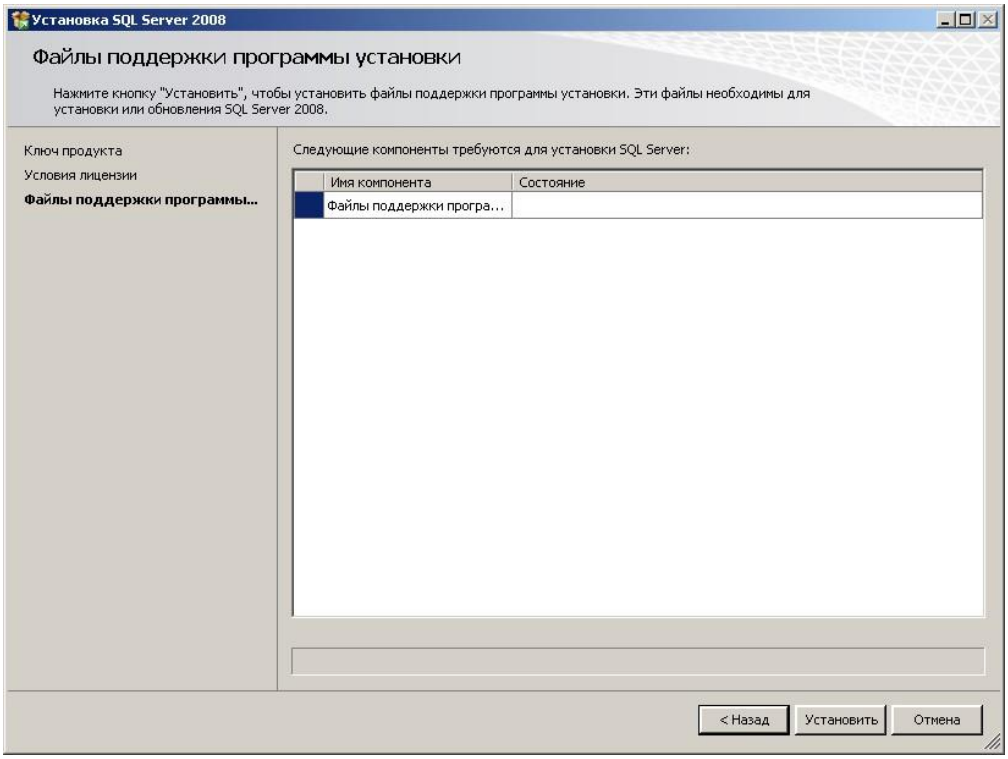

Рисунок 2.12

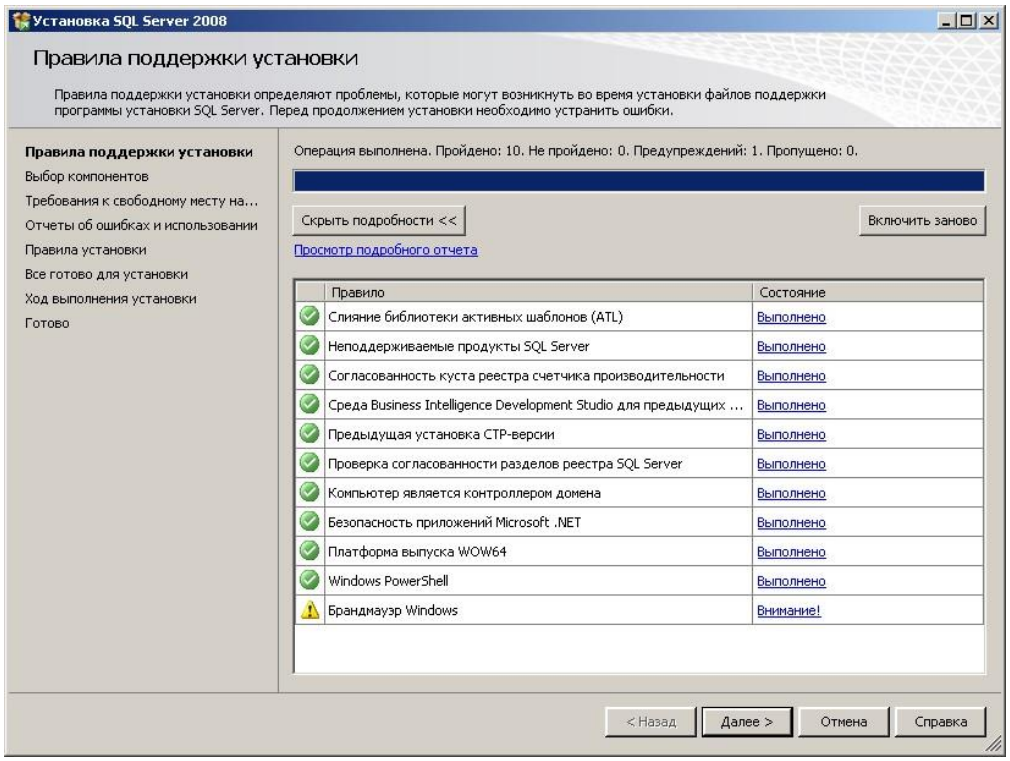

Рисунок 2.13

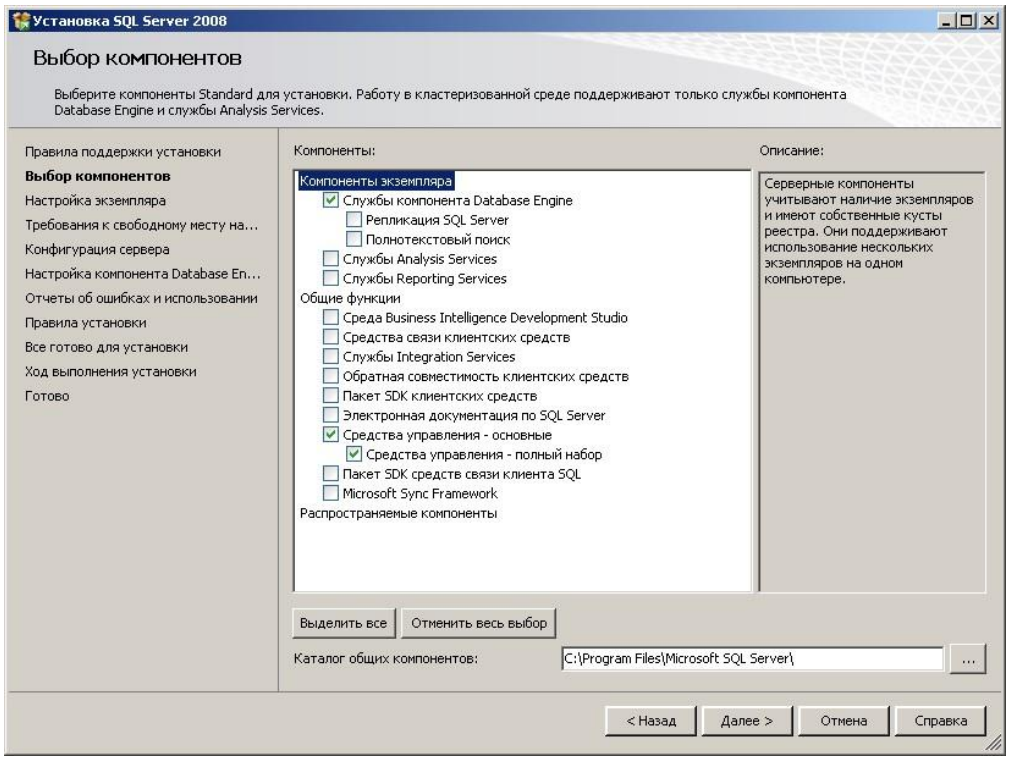

Рисунок 2.14

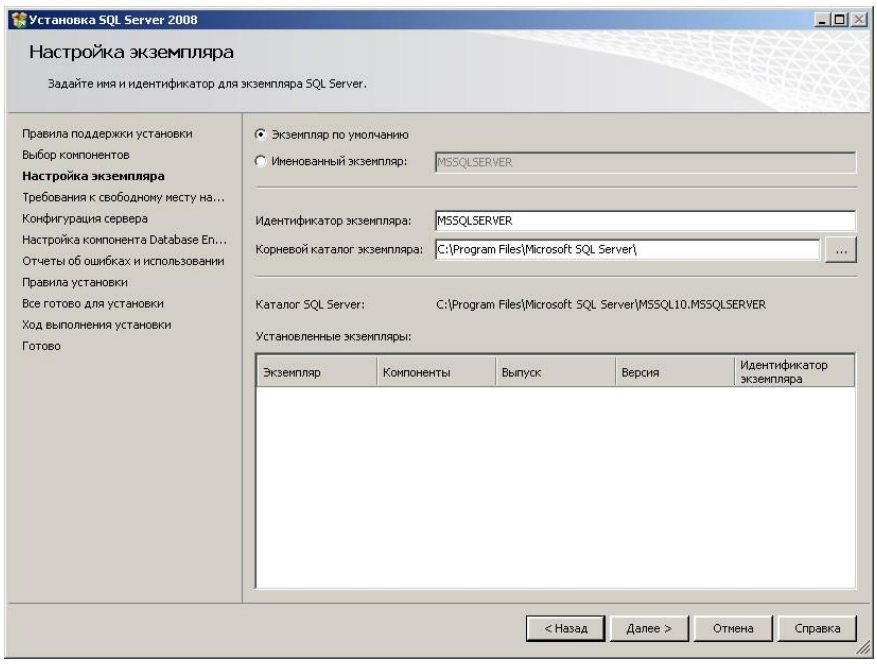

Рисунок 2.15

Далее программа установки проверит наличие свободного места на диске (рисунок 2.16). Необходимо нажать кнопку «Далее >».

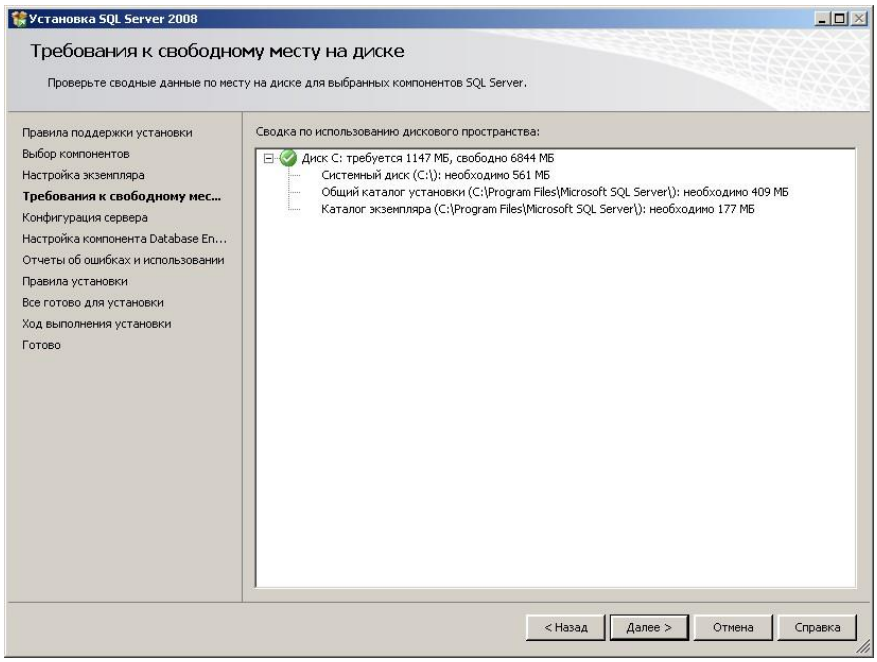

Рисунок 2.16

В следующем окне (рисунок 2.17) необходимо выбрать параметры учетных записей служб. Для служб «Агент SQL Server» и «SQL Server Database Engine» в качестве имени учетной записи необходимо выбрать «NT AUTHORITY\NETWORK SERVICE», а тип запуска – «Авто». После этого нажать кнопку «Далее >».

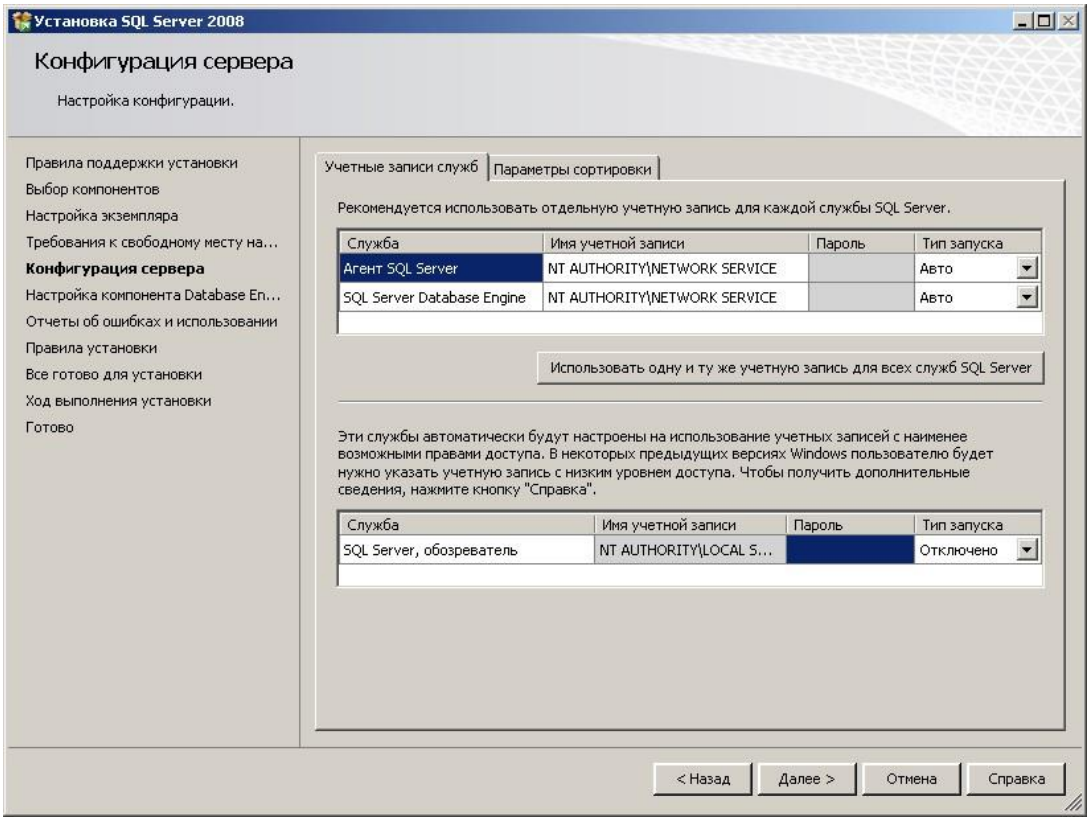

Рисунок 2.17

Далее программа установки предложит выбрать режим проверки подлинности (рисунок 2.18). Необходимо выбрать «Смешанный режим (проверка подлинности SQL Server и Windows)». Далее необходимо ввести пароль, который в дальнейшем потребуется ввести при установке СОА «Форпост». Затем необходимо назначить администратора SQL Server, которым может выступать текущий пользователь. Для этого необходимо

нажать кнопку «Добавить текущего пользователя». После этого необходимо нажать кнопку «Далее >».

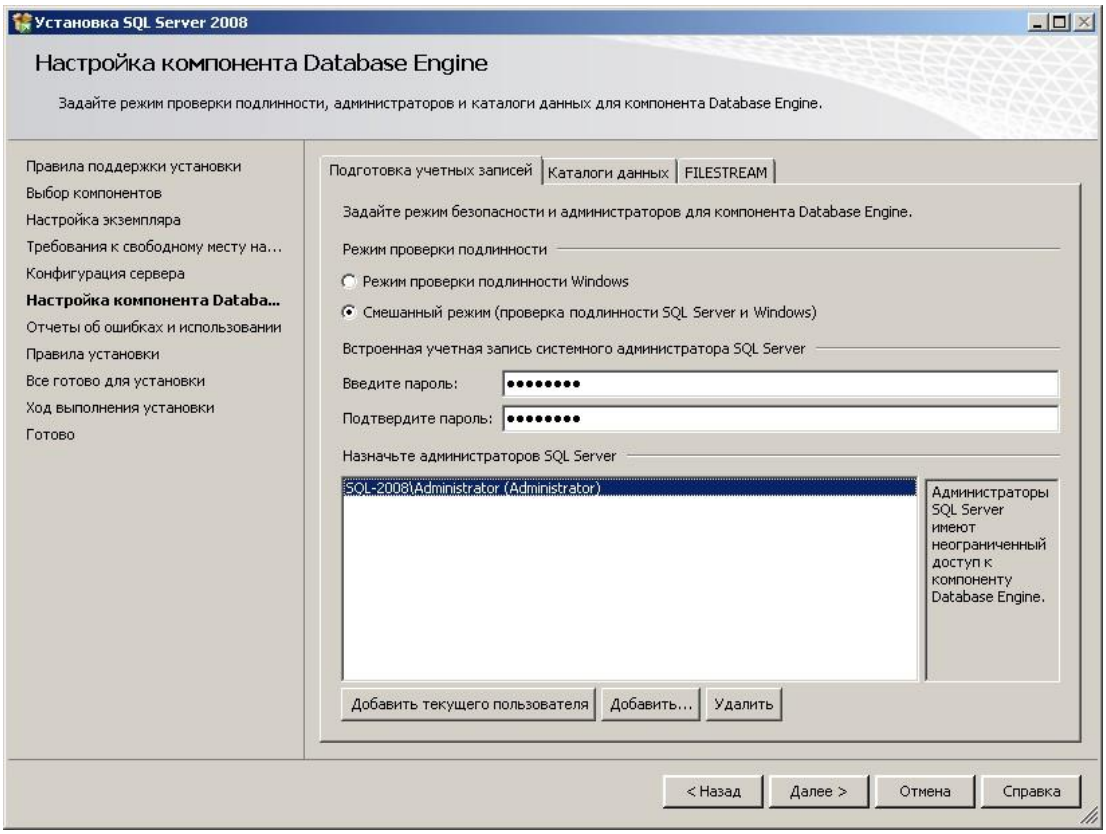

Рисунок 2.18

В следующих окнах (рисунок 2.19 и 2.20) необходимо оставить все параметры в значениях по умолчанию и нажимать кнопку «Далее >».

В следующем окне приведены параметры установки (рисунок 2.21). Необходимо их проверить и нажать кнопку «Установить». Дождитесь окончания установки (рисунок 2.22).

В следующем окне (рисунок 2.23) приведена информация по результатам установки. Все значки напротив устанавливаемых компонентов должны быть зеленого цвета. Необходимо нажать кнопку «Далее >».

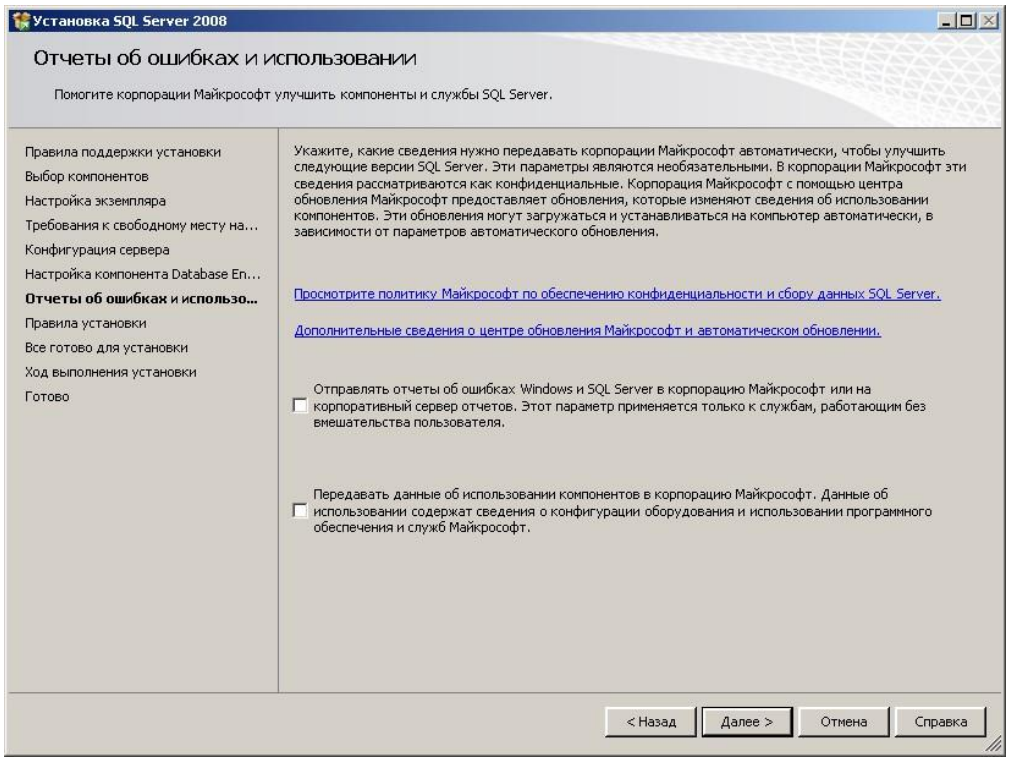

Рисунок 2.19

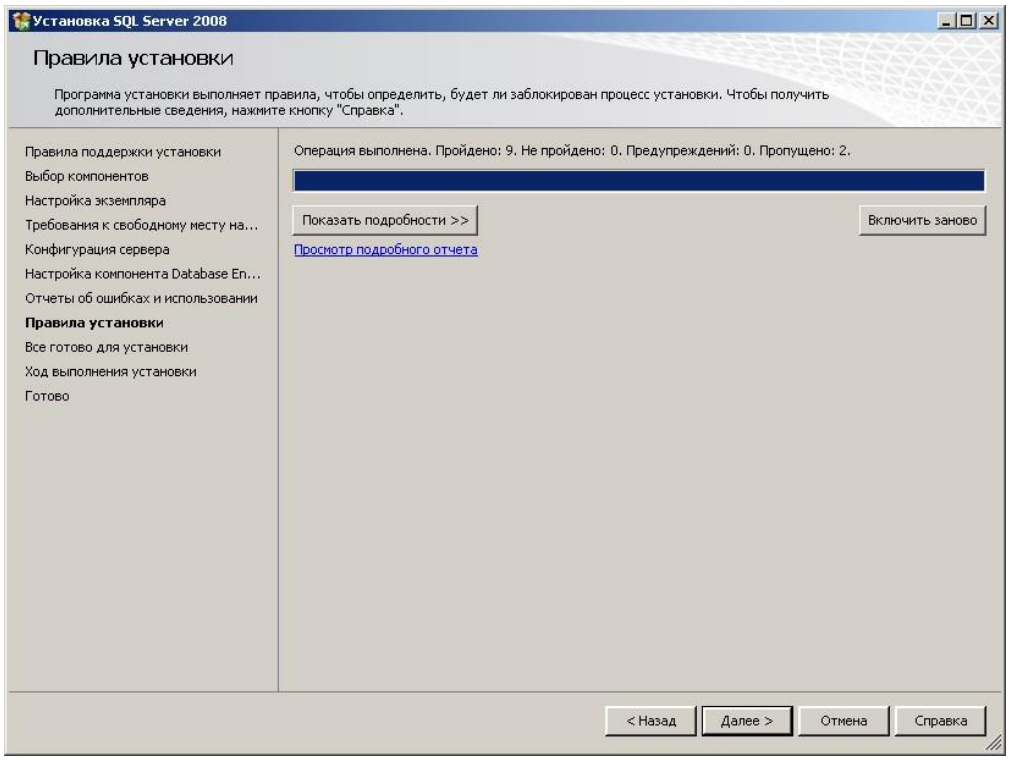

Рисунок 2.20

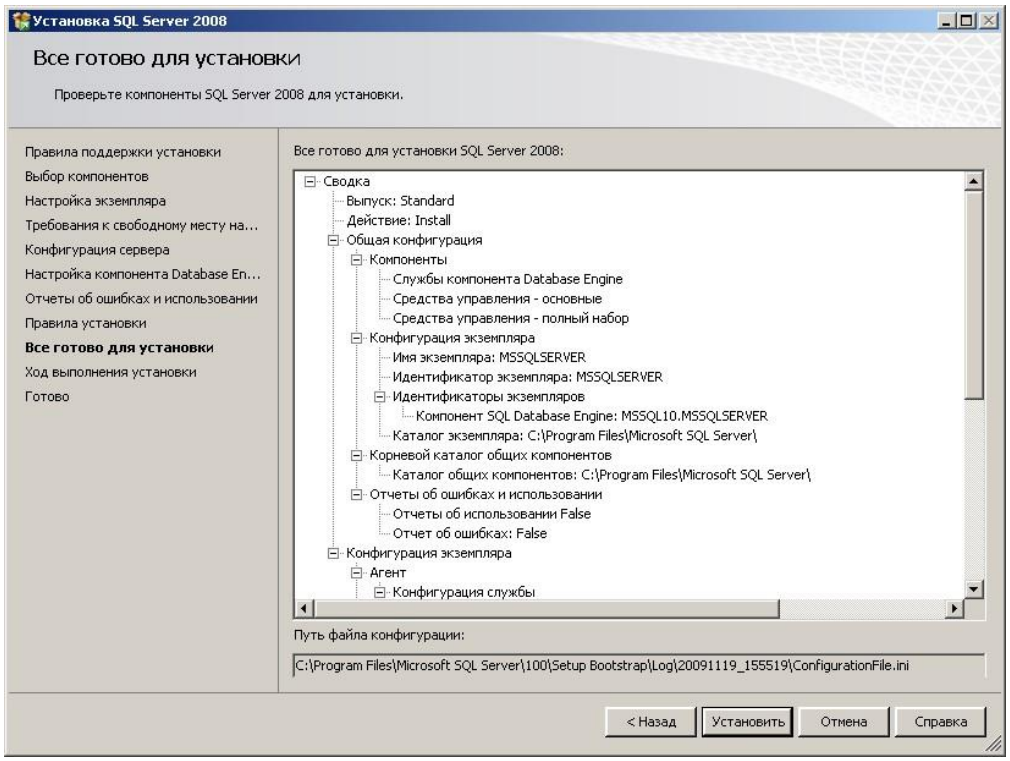

Рисунок 2.21

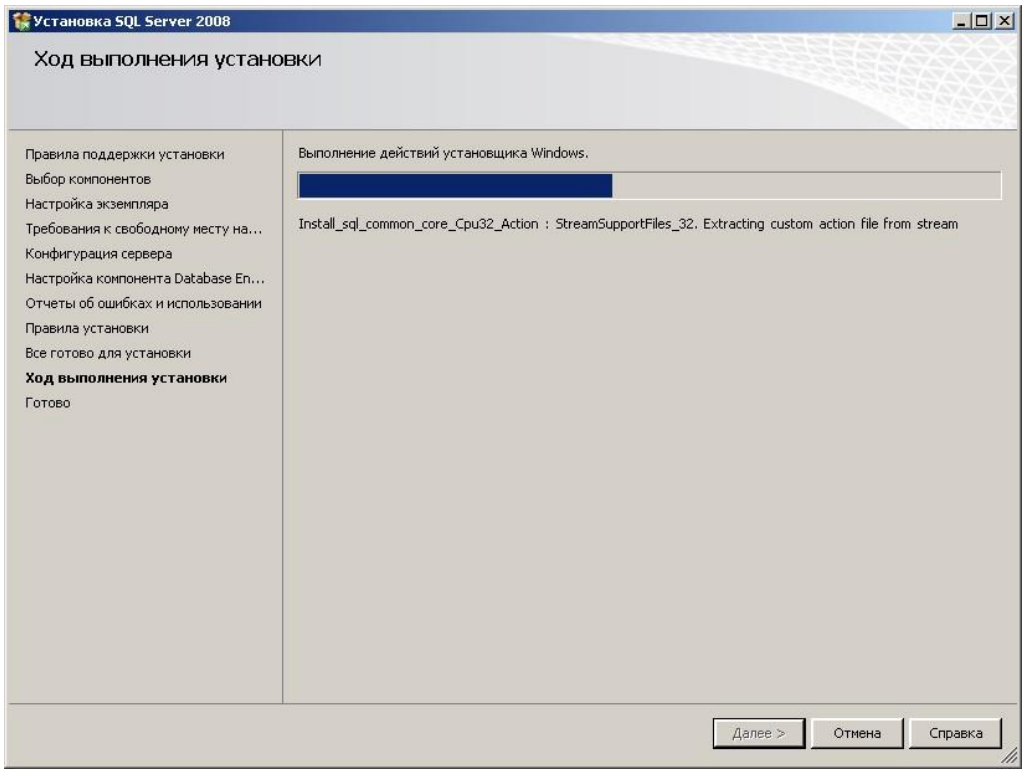

Рисунок 2.22

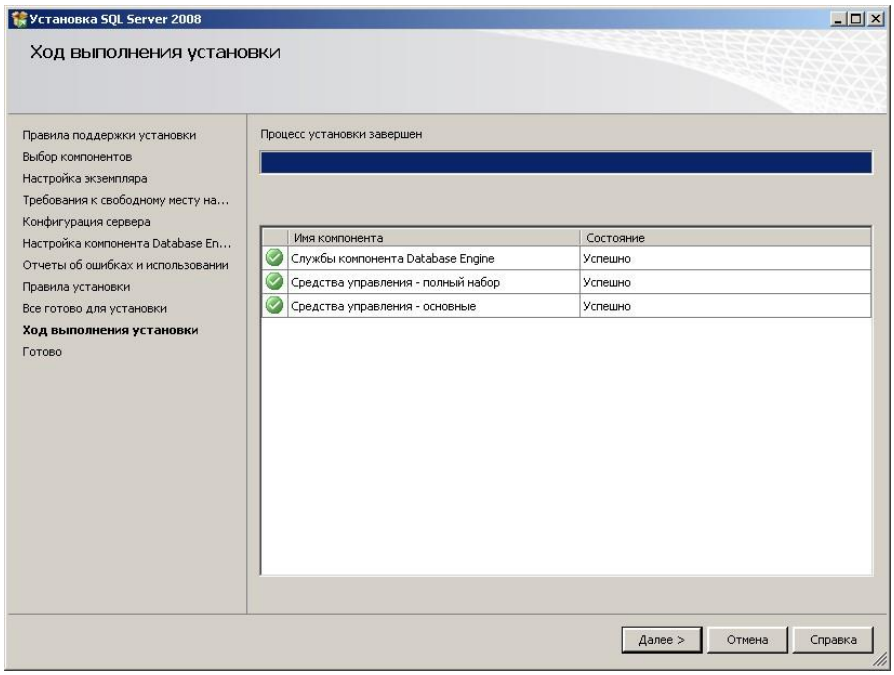

Рисунок 2.23

Далее появится окно, сообщающее об успешности установки (рисунок 2.24). Необходимо нажать кнопку «Закрыть».

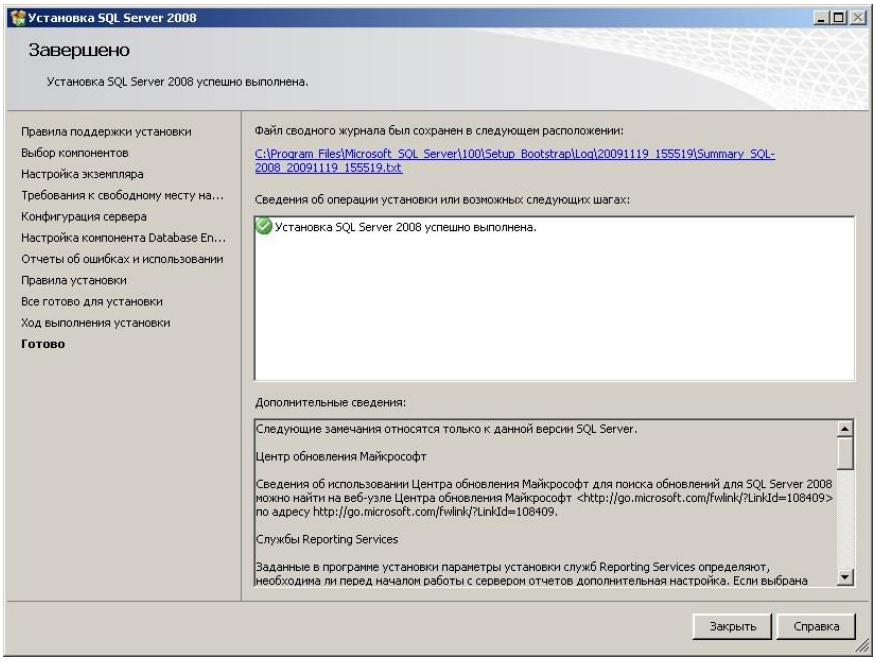

Рисунок 2.24

ЗАКЛЮЧЕНИЕ

Стремительное развитие ИСОД МВД России провоцирует возникновение новых угроз, своевременное реагирование на которые становится главной задачей подсистемы информационной безопасности.

Поэтому в методических рекомендациях представлен анализ основных этапов построения комплексной системы обнаружения, реагирования и предотвращения возникновения инцидентов безопасности. В настоящее время совокупность разрозненных технических решений и отсутствие централизованного, регламентирующего создание такого механизма, документа не позволяет на должном уровне обеспечивать обработку инцидентов информационной безопасности и предотвращать их возникновение, но описанные в работе подходы позволят приблизиться к созданию подобной системы.

Реализация регламента, описывающего все этапы организации информационного обмена на разных уровнях телекоммуникационной системы, а также реализация многоэтапной системы управления инцидентами информационной безопасности будут способствовать повышению эффективности работы подсистемы информационной безопасности ИСОД МВД России в целом.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Рябко Б. А. Криптографические методы защиты информации: учебное пособие: рек. УМО по образ. / Б. А. Рябко, А. Н. Фионов. - Москва: Горячая линия - Телеком, 2014. - 229 с.: ил.

2. Зайцев, А. П. Технические средства и методы защиты информации: учебное пособие: рек. Мин. образ. и науки РФ / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов ; под ред. А.П. Зайцева и А.А. Шелупанова. - 7-е изд. - Москва: Горячая линия - Телеком, 2014. - 442 с.: ил.

3. Алферов А. Основы криптографии: учебное пособие: рек. Мин. образ. и науки РФ / А. Алферов, А. Зубов, А. Кузьмин, А. Черемушкин – Москва: Гелиос АРВ, 2005. – 480 с.: ил.

4. Техническая документация «DioNIS TS/FW/16000/KB2», «DioNIS MS».

5. Информационная безопасность открытых систем [Текст] : [учебник]: доп. М-вом образования РФ. Т.2 : Средства защиты в сетях / С. В. Запечников [и др.]. - М. : Горячая линия - Телеком, 2008. - 558 с. : ил. - Лит. : с. 550-553.

6. Основы построения систем и сетей передачи информации [Текст] : [учебное пособие]: рек. УМО по образованию / В. В. Ломовицкий [и др.] ; под ред. В.М. Щекотихина . - М. : Горячая линия-Телеком, 2005. - 382 с. : ил.

7. Башлы П. Н. Современные сетевые технологии [Текст] : учеб. пособие : рек. УМО по образованию / П. Н. Башлы. - М. : Горячая линия - Телеком, 2006. - 334 с.

8. Битнер В. И. Сети нового поколения - NGN [Текст] : учебное пособие: рек. УМО вузов по универ. политех. образ. / В. И. Битнер, Ц. Ц. Михайлова. - М. : Горячая линия - Телеком, 2011. - 226 с. : ил.

9. ViPNet Administrator: практикум [Текст] : официальный учебный курс по организации виртуальных защищенных сетей ViPNet / Чефранова А. О. и др. ; под ред. А.О. Чефрановой. - 5-е изд., перераб. - Москва : Горячая линия - Телеком, 2012. - 192 с. : ил. - (Б-ка специалиста по информационной безопасности. Вып.1).

10. Анин Б.Ю. Защита компьютерной информации. – СПб. BXB – Петербург, 2000. –384с.