МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

В.А. Заляжных
А.В. Гирик

ЭКСПЕРТНЫЕ СИСТЕМЫ КОМПЛЕКСНОЙ ОЦЕНКИ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ СИСТЕМ

Учебно-методическое пособие

Санкт-Петербург

2014

Заляжных В.А., Гирик А.В. Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем. – СПб: Университет ИТМО, 2014. – 136с.

В учебно-методическом пособии на основании анализа известных инцидентов информационной безопасности и рекомендаций экспертов изложены вопросы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем. Определены требования к программному и аппаратному обеспечению, практические рекомендации по конфигурированию систем. Так же рассмотрены вопросы защиты от атак, связанных с обманом человека.

Рецензенты: д.т.н. СНС В.Г. Швед
к.т.н. доцент Г.П. Жигулин

Рекомендовано Ученым советом Института комплексного военного образования СПб НИУ ИТМО протокол №4 05.05.2014 в качестве учебного пособия для бакалавров, магистрантов и аспирантов, обучающихся по направлению подготовки «Информационная безопасность».

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Заляжных В.А., Гирик А.В. Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем. – СПб: Университет ИТМО, 2014. – 136с.

В учебно-методическом пособии на основании анализа известных инцидентов информационной безопасности и рекомендаций экспертов изложены вопросы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем. Определены требования к программному и аппаратному обеспечению, практические рекомендации по конфигурированию систем. Так же рассмотрены вопросы защиты от атак, связанных с обманом человека.

Рецензенты: д.т.н. СНС В.Г. Швед
к.т.н. доцент Г.П. Жигулин

Рекомендовано Ученым советом Института комплексного военного образования СПб НИУ ИТМО протокол №4 05.05.2014 в качестве учебного пособия для бакалавров, магистрантов и аспирантов, обучающихся по направлению подготовки «Информационная безопасность».

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.

Защита информации – это обширная область знаний, которая включает в себя правовые, организационные, технические аспекты. Практически каждый информационного объект требует особого подхода, когда требуется обеспечить безопасность. В данном пособии рассматриваются вопросы защиты информации при работе с персональным компьютером.

В первой главе изложены основные понятия и принципы информационной безопасности, которые применимы для защиты персонального компьютера.

Во второй главе рассматривается безопасность операционной системы: описаны типичные информационные угрозы, характерные для современных систем, изложены методические рекомендации по конфигурированию систем безопасности, описаны примеры организации шифрования и многофакторной аутентификации.

Третья глава содержит краткие рекомендации по защите информации при использовании сети интернет. Следует отметить, что в данном пособии не рассматриваются вопросы обеспечения сетевой безопасности (конфигурирование маршрутизаторов, сетевых экранов, серверов, проектирование сети и т.п.).

В последней, четвертой главе рассматриваются угрозы безопасности персонального компьютера, связанные с возможностью понижения безопасности системы с помощью обмана человека, т.е. *социальной инженерии*.

ГЛАВА 1. ОСНОВЫ

1.1. Инцидент информационной безопасности

Понятие

Вне зависимости от методов защиты в работе любой автоматизированной системы происходят непредусмотренные события. Они могут быть вызваны ошибками программирования, аппаратным сбоем, действиями человека или другими причинами. В случае если такое событие оказывает значительное влияние на информационную безопасность защищаемого объекта, такое событие называют **инцидентом информационной безопасности.**

Законодательство

ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

Инцидент информационной безопасности (инцидент ИБ) - Одно или серия нежелательных или неожиданных событий в системе информационной безопасности, которые имеют большой шанс скомпрометировать деловые операции и поставить под угрозу защиту информации.

Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 "Обеспечение ИБ организаций банковской системы РФ. Общие положения". Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года №Р705.

Инцидент информационной безопасности - Событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

Примечания.

1. Реализация угрозы ИБ – реализация нарушения свойств ИБ информационных активов организации банковской системы Российской Федерации.
2. Нарушение может вызываться источниками угроз ИБ: либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств, природными факторами, например, пожаром или наводнением), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов.

1.2. Терминология

Термин	Определение
Доступ	В контексте конфиденциальности под доступом понимают имеющуюся у пользователя возможность просматривать и изменять свои личные данные, а также проверять их правильность и полноту. Управление доступом входит в «Принципы добросовестного использования информации».
АВПО	Антивирусное программное обеспечение, антивирус. Приложения, которые осуществляют поиск вирусов, червей и других вредоносных программ и предпринимают при их обнаружении соответствующие меры. В число возможных мер входит блокировка зараженных файлов, очистка зараженных файлов или компьютеров и уведомление пользователя об обнаружении зараженной программы.
Атака	Умышленная попытка нарушить безопасность компьютерной системы или лишить других пользователей возможности работать с ней.
Аутентификация	Проверка подлинности. Процесс проверки учетных данных пользователя, компьютерного процесса или устройства. Для проверки подлинности необходимо, чтобы пользователи, процессы и устройства предоставляли данные, подтверждающие, что они являются теми, за кого себя выдают. В качестве учетных данных часто используются цифровые подписи, смарт-карты, биометрические данные и сочетания имени пользователя и пароля.
Авторизация	Процесс предоставления пользователю, компьютерному процессу или устройству доступа к некоторым данным, службам или функциям. При авторизации используются учетные данные запросившего доступ пользователя, компьютерного процесса или устройства, прошедшие проверку подлинности. См. 2.5.
Вычислительные ресурсы	Вычислительными ресурсами называются возможности, обеспечиваемые компонентами вычислительной системы, расходуемые (занимаемые) в процессе её работы. Как вычислительным ресурсам относятся: процессорное время, память (оперативная и виртуальная), место на жёстком диске (постоянная память), пропускная способность сети.
ВПО	Вредоносное программное обеспечение. Программы, которые при запуске выполняют действия, помогающие атакующему осуществить его злые намерения. Примерами таких программ могут служить вирусы, черви и «троянские кони». См. 2.2.2.
Пароль	Строка знаков, вводимая пользователем для подтверждения своей подлинности при входе в сеть или локальную систему. См. 2.2.1.
Разрешения	Права на выполнение операций над тем или иным общим ресурсом, таким как файл, каталог или принтер. Разрешения предоставляются администратором отдельным учетным записям пользователей или административным группам.
MITM-атака	(англ. Man in the middle — «человек посередине») Ситуация, когда криптоаналитик (атакующий) способен читать и видоизменять по своей воле сообщения, которыми обмениваются корреспонденты, причём ни один из последних не может догадаться о его присутствии в канале. Метод компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет активное вмешательство в протокол передачи, удаляя, искажая информацию или навязывая ложную.
XSRF-атака	(англ. Cross Site Request Forgery — «Межсайтовая подделка запроса») Вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP, подразумевающий выполнение поддельного запроса на другой сервер от имени жертвы.
DoS-атака	(англ. Denial of Service — «отказ в обслуживании») атака на вычислительную систему с целью создания таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам, либо этот доступ затруднён.

Brute force	Полный перебор (или метод «грубой силы», англ. brute force) — метод решения математических задач. Относится к классу методов поиска решения исчерпыванием всевозможных вариантов. Сложность полного перебора зависит от количества всех возможных решений задачи. Данный способ широко применяется для взлома парольной аутентификации. В криптографии на вычислительной сложности полного перебора основывается оценка криптостойкости шифров. В частности, шифр считается криптостойким, если не существует метода «взлома» существенно более быстрого чем полный перебор всех ключей. Криптографические атаки, основанные на методе полного перебора, являются самыми универсальными, но и самыми долгими.
Сканер портов (ПО для сетевого сканирования)	Программное средства, разработанные для поиска хостов сети, в которых открыты нужные порты. Эти программы обычно используются системными администраторами для проверки безопасности их сетей и злоумышленниками для взлома сети. Может производиться поиск как ряда открытых портов на одном хосте, так и одного определённого порта на многих хостах. Последнее характерно для деятельности ряда сетевых червей. Сканирование портов может являться первым шагом в процессе взлома или предупреждения взлома, помогая определить потенциальные цели атаки. С помощью соответствующего инструментария путем отправления пакетов данных и анализа ответов могут быть исследованы работающие на машине службы (Web-сервер, FTP-сервер, mail-сервер, и т. д.), установлены номера их версий и используемая операционная система.

1.3. Возможные потери от атак злоумышленников

Атаки злоумышленников могут быть направлены на кражу любой информации, из которой можно извлечь финансовую выгоду, так же целью может быть снижение доступности важной информации или другая деструктивная деятельность.

Средний размер ущерба в результате одного инцидента[1] можно оценить в 14 тыс. долларов для малых и средних компаний и 695 тыс. долларов для крупных российских организаций. Такую оценку приводят аналитики компании B2B International и «Лаборатория Касперского» в совместном исследовании по информационной безопасности бизнеса[2].

К столь большим потерям приводят три основных фактора: вынужденный простой, упущенные возможности для бизнеса (включая потерю контрактов из-за кибератаки), а также расходы на дополни-

[1] Здесь и далее по тексту под словом «инцидент» подразумевается термин «инцидент информационной безопасности».

[2] Исследование «Информационная безопасность бизнеса», проведенное «Лабораторией Касперского» и B2B International в 2013 году. В исследовании приняли участие более 2895 IT-специалистов из 24 стран мира.

тельные услуги различных специалистов. По данным опроса, компаниям, относящимся к малому и среднему бизнесу вынужденный простой обходится в среднем в 13 тыс. долларов, а крупным организациям — в 791 тыс. долларов. Упущенные возможности также выражаются в финансовых потерях, средний размер которых для малых и средних компаний составил 16 тыс. долларов, а максимально возможный ущерб, по оценкам опрошенных, мог достигать 375 тыс. долларов. Что касается дополнительных услуг различных специалистов, в среднем общие расходы на них достигают 6,6 тыс. долларов для небольших компаний, и 26 тыс. долларов для крупных корпораций.

Кроме того, по данным опроса, один инцидент с утечкой данных в 58% случаев вызвал временную утрату доступа к важной деловой информации. А почти в четверти случаев (24%) инцидент привел к потере важных деловых контрактов и упущенным возможностям для развития бизнеса.

«Ущерб в денежном выражении более чем нагляден, но не стоит также забывать и о сопутствующих рисках, к примеру, потере деловой репутации компании и о том, что помимо финансовых издержек, вызванных непосредственно самим инцидентом, компании часто в таком случае в экстренном режиме расходуют средства на ряд дополнительных защитных мер, призванных, в том числе, снизить вероятность возникновения подобных инцидентов в будущем», — комментирует Кирилл Керценбаум, сотрудник «Лаборатории Касперского».

1.4. Требования к защите информации

N 149-ФЗ от 27 июля 2006 года в редакции от 28.12.2013.
ФЕДЕРАЛЬНЫЙ ЗАКОН ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ. Статья 16, пункт 4.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, мо-

дифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

1.5. Основные меры обеспечения информационной безопасности компьютерных систем

Обеспечение доверенной загрузки. Загрузка ОС только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации / аутентификации пользователя.

Идентификация и аутентификация. Субъект проходит процедуру аутентификации, и если аутентификация успешна, то информационная система на основе факторов аутентификации определяет идентификатор субъекта. При этом достоверность идентификации полностью определяется уровнем достоверности выполненной процедуры аутентификации (проверка подлинности пользователя путём проверки введённого им пароля; подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя; проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла). Учитывая степень доверия и политику безопасности систем, проводимая проверка подлинности может быть односторонней или взаимной. Обычно она проводится с помощью криптографических способов.

Управление доступом. Политика безопасности определяет права субъектов (например, пользователей системы) на совершение действий над объектами данных. Для исполнения политики безопасности требуется некая система для управления доступом к объектам. Такая система разграничения доступа субъектов к объектам рассматривается в качестве главного средства защиты от несанкционированного доступа к информации.

Ограничение программной среды. Для всех узлов сети, программных и аппаратных средств должно действовать правило: запрещено всё, что не разрешено. Т.е. доступ к какому-либо объекту системы должен предоставляться только при наличии соответствующего правила. Этот принцип реализуется с помощью административных, про-

граммных и аппаратных средств. При этом основной функцией системы ИБ является разрешение, а не запрещение каких-либо действий, что позволяет допускать только известные безопасные действия. При формировании политики безопасности следует убедиться в отсутствии избыточных прав доступа к данным и к функциональным возможностям программ. Такие ограничения, тем не менее, не должны мешать выполнению работы.

Защита машинных носителей информации. Если защищаемая информация размещается на машинных носителях информации, то она должна быть защищена с помощью криптографических средств. Так же следует вести учёт машинных носителей информации и исключить возможность использования неучтенных носителей.

Обеспечение целостности данных. Резервное копирование (англ. backup) – это процесс создания копии, предназначенной для восстановления данных в случае их повреждения. Резервная копия должна храниться в надёжном месте. При необходимости используется система автоматического восстановления.

Регистрация событий. Отчётность – важный аспект информационной безопасности. Любое взаимодействие с информационной системой должно проходить под полным контролем. Для этого создаётся файл регистрации[3], который не могут редактировать пользователи; в нём автоматически создаются записи о каждой операции, выполняемой программой, с указанием времени и идентификатора пользователя, инициировавшего операцию. Данные журналы регулярно анализируются с целью выявления угроз информационной безопасности. Так же следует предусмотреть автоматическую систему оповещения об инцидентах информационной безопасности, для чего применяют систему обнаружения вторжений (СОВ).

Активная защита. Подразумевает использование Антивирусного ПО и/или средств обнаружения (предотвращения) вторжений.

Контроль и анализ защищенности данных. Данный принцип подразумевает формирование единой политики безопасности и контроль за ее исполнением. Регулярно должны проводиться мероприятия по комплексному анализу защищенности данных, тестирование

---

[3] Равнозначно могут применяться термины протокол, журнал или лог (от англ. Log)

работоспособности системы защиты. Так же внедряются средства для обеспечения целостности информационной системы и данных, резервное копирование и автоматическое восстановление.

Управление конфигурацией информационной системы и системы защиты. Необходимо использовать только те программные и аппаратные средства, которые отвечают современным стандартам по защите информации. Для этого необходимо предварительно изучать спецификацию всех внедряемых средств. Безопасность не должна обеспечиваться через неясность. Попытки защитить информационную систему от угроз ИБ путем усложнения и скрытия слабых мест системы защиты, оказываются в конечном итоге несостоятельными и только отсрочивают успешную хакерскую, вирусную или инсайдерскую атаку. При разработке и внедрении ИС следует использовать только те программные и аппаратные средства защиты информации, которые прошли исследование с целью выявления изъянов или скрытого функционала. Для примера, этому принципу не соответствуют такие популярные программы, как Skype или ОС Windows: их использование при работе со сведениями ограниченного доступа допустимо только в комплексе с дополнительными средствами защиты. При этом следует помнить, что данный принцип информационной безопасности не означает простоту архитектуры и снижение функциональности ИС.

1.6. Уровни безопасности

Меры, которые необходимо предпринимать для обеспечения безопасности ИС можно разделить на уровни безопасности таким образом, что каждый последующий уровень обеспечивает бóльшую степень защищенности, однако он может оказаться бесполезным, если не обеспечены предыдущие.

1. Оборудование

Изъяны в протоколах, драйверах или микропрограммах могут быть использованы для перехвата данных или для обхода аутентификации, поэтому необходимо уделять особое внимание выбору оборудования и конфигурированию. Так же, по мере необходимости рекомендуется применять аппаратные средства криптографии.

2. Программное обеспечение

Практически во всех программах присутствуют уязвимости. Чтобы снизить вероятность атаки с использованием уязвимости, необходимо регулярно устанавливать рекомендуемые обновления. Не следует признавать безопасными программы, архитектура которых не из-

вестна или программы, в которых неоднократно были обнаружены критические уязвимости.

3. Антивирусное ПО

Несмотря на то, что наиболее опытные взломщики не используют ВПО, которое может быть обнаружено антивирусной программой, при работе с небезопасными сетями (напр., интернет) или с файлами из небезопасных источников (напр., с домашних компьютеров сотрудников) вероятность случайного заражения всё равно высока.

4. Разграничение доступа

Чтобы не допустить свободного распространения защищаемых данных и понизить риск инсайдерской атаки, вводятся правила доступа к информационным объектам (файлы, каталоги, устройства, хосты, сетевые порты и т.д.); они должны быть закреплены не только в виде запрограммированных правил, но и административно, то есть в виде документа (Положение о разрешительной системе допуска к информационным ресурсам).

5. Межсетевой экран

Основная задача межсетевого экрана (равнозначно могут применяться термины: сетевой экран, файервол, брандмауэр) – не пропускать пакеты, не подходящие под критерии, определённые в конфигурации. Существует множество программных и аппаратных решений, выполняющих эту функцию, к ним относятся управляемые коммутаторы, шлюзы сеансового (напр. SOCKS) и прикладного (прокси-сервер) уровня и т.д. Типичное применение файервола – фильтрация доступа к заведомо незащищенным узлам сети.

6. Система предотвращения (обнаружения) вторжений

Компьютерные взломщики, как правило, используют схожие методы проникновения в информационную систему; для того чтобы вовремя обнаружить такие действия, применяют систему предотвращения вторжений, которая постоянно анализирует сетевую активность и предотвращает подозрительные действия (напр., повышение прав доступа или сетевое сканирование). В некоторых случаях, во избежание негативных последствий от ложного срабатывания, невозможно дать такой программе полномочия по предотвращению подозрительной активности: в таком случае говорят о системе *обнаружения* вторжений, которая лишь информирует администратора об инцидентах.

7. Контроль физического доступа

Никогда нельзя забывать, что получить физический доступ к компьютеру обычно намного проще и дешевле, чем нанимать хакера, который его взломает.

8. Осведомлённость пользователей

Большинство уязвимостей появляется от незнания пользователями основ безопасности. Для пользователя все меры защиты информации выглядят лишними «помехами в работе». Поэтому необходимо проводить обучение пользователей, а так же на предприятиях рекомендуется вводить документ, описывающий правила пользования ИС, который должен подписать каждый пользователь ИС.

9. Политика безопасности

Основой информационной безопасности является политика безопасности, которая подробно описывает все руководящие правила, принципы, процедуры и практические приёмы в области безопасности, которые должны применяться в организации. Так же следует постоянно проводить мониторинг и анализ всех операций в информационной системе с целью выявления потребностей в обновлении политики безопасности.

10. Сертификация

В случае целесообразности (это означает: если потеря защищаемых данных влечет за собой огромные финансовые потери) необходимо применять оборудование и программное обеспечение, соответствующее требованиям безопасности в области информационных технологий и обладающее сертификатами об этом.

Для того чтобы убедиться в безопасности ИС, рекомендуется привлекать для аудита организации, специализирующиеся на информационной безопасности. Все рекомендации должны формироваться только в виде отчета: не следует перекладывать конфигурирование средств защиты на сторонние организации. Так же не следует допускать возможности ознакомления с защищаемой информацией. Доверенность той или иной организации в области обеспечения информационной безопасности подтверждается сертификатами и лицензиями.

ГЛАВА 2. ЗАЩИТА ОПЕРАЦИОННОЙ СИСТЕМЫ

2.1. Безопасность системы

Все действия над файлами и устройствами производятся с помощью операционной системы, следовательно получение контроля над ней – это основная цель злоумышленника. Поэтому операционная система компьютера должна иметь следующие базовые средства защиты:

1. Идентификация и аутентификация. Ни один пользователь не может начать работу с ОС, не идентифицировав себя и не предоста-

вив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.

2. Разграничение доступа. Каждый пользователь системы имеет только те привелегии, которые ему предоставлены в соответствии с текущей политикой безопасности.

3. Отчётность. ОС регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.

4. Управление политикой безопасности. ОС имеет удобные средства для установки правил взаимодействия с файлами и устройствами.

5. Криптографические функции. Криптографические средства используются в ОС повсеместно: для проверки цифровых подписей, для обеспечения аутентификации, для сокрытия информации и т.д.

В этой главе мы рассмотрим основные угрозы безопасности системы и методы защиты на примере ОС Windows.

2.2. Угрозы безопасности системы

Можно разделить угрозы безопасности ОС на четыре типа:

А) Использование уязвимостей самой ОС.

Некоторые операционные системы содержат возможность произведения несанкционированных действий, причем такие возможности могут быть заложены в ОС намеренно: например, для противодействия терроризму. Однако, применение подобных уязвимостей маловероятно.

Нельзя забывать, что большинство программ содержит неизвестные уязвимости, которые не устраняются с помощью обновлений: такие уязвимости называют 0day (zero-day, уязвимость нулевого дня). Специалист по безопасности должен настраивать систему так, чтобы абсолютное большинство таких уязвимостей невозможно было использовать. Это достигается с помощью продуманной политики безопасности и системы обнаружения вторжений.

Б) Ошибочное конфигурирование средств защиты.

Политика безопасности должна быть продуманной, логичной и очевидной. Все правила должны применяться постоянно. Нельзя допускать «временных решений», понижающих безопасность системы.

В) Нарушение процедуры аутентификации.

Любой аутентификатор может быть украден или подделан: пароль можно подобрать, токен – скопировать, существуют способы под-

делки биометрических атрибутов аутентификации. Для повышения надежности системы рекомендуется использовать многофакторную аутентификацию.

Г) Внедрение вредоносной программы.

Большинство успешных и причинивших наибольший ущерб атак не обошлось без использования специальных алгоритмов, которые выполнялись операционной системой.

2.2.1. Взлом паролей

Пароль – это текстовая строка, известная только своему владельцу, это наиболее распространенный аутентификатор.

Безопасность парольной аутентификации обеспечивается следующими мерами:

1) Защита механизма аутентификации. Необходимо убедиться, что посторонний не может вносить изменения в механизм аутентификации. (Например, в Windows 98 присутствовала критическая уязвимость, которая через окно справки позволяла вызвать ошибку в системе аутентификации и продолжить загрузку системы). В системе, обеспечивающей аутентификацию, хранится не сам пароль, а его цифровой «отпечаток»: хэш фиксированной длины, для того чтобы пароли пользователей были недоступны злоумышленнику, получившему доступ к файлам системы аутентификации.

2) Сохранность хранилища паролей. Пароли можно хранить только в зашифрованном виде, однако лучше использовать пароли, которые легко запомнить.

3) Защита от перебора. Недопустима ситуация, при которой доступ можно получить с помощью подбора пароля. Для защиты применяется ввод дополнительного времени между попытками ввода пароля и самоблокирование в случае многократно введенного неверного пароля. Данные меры могут оказаться бессмысленны в том случае, если пароль является ключом для криптографического алгоритма и атакующий владеет фрагментом зашифрованного сообщения: в этом случае подбор пароля может быть осуществлен на вычислительных мощностях атакующего и защитить информацию поможет только достаточно надежный пароль.

4) Регулярная принудительная смена паролей. Смена паролей необходима для дополнительной защиты от перебора и для того, чтобы предотвратить распространение пароля («Ой, напомни, какой там у Маши пароль?»). Обратите внимание, что в определенных случаях

внедрение такого мероприятия может понизить информационную безопасность: пользователи могут начать использовать простые пароли или записывать их в неподходящем месте.

5) Надёжный пароль. Надёжность пароля определяется его длиной и непредсказуемостью.

Не используйте в качестве паролей простые фразы и слова, так как они могут содержаться в специальных словарях: вместо этого используйте фразы, бессмысленные для посторонних (например, составьте пароль из названий ваших любимых литературных произведений, пропустив гласные, а затем запишите гласные подряд, в верхнем регистре: «Nrmncr1984FghtClbEUOAEIU»). Наиболее важные объекты должны быть защищены уникальным паролем (некоторые взломщики в поисках пароля к защищенной системе могут взломать системы, используемые сотрудником в личных целях). Не следует прибегать к простой ротации паролей (Пароль1, Пароль2, Пароль3, …). По возможности используйте все доступные символы.

Большинство паролей состоят из 6-8 символов, содержат цифры только в конце или начале, целиком состоят из цифр, содержат от нуля до двух заглавных букв и/или состоят из простых распространенных слов. Эти особенности могут быть использованы при составлении порядка перебора символов для ускорения подбора пароля.

Исходя из сложности шифрующего алгоритма и возможной вычислительной мощности системы, производящей перебор, определяется потенциальная скорость перебора. На ее основе устанавливается минимальная длина пароля и срок действия пароля таким образом, чтобы теоретическое время подбора пароля было меньше срока его действия. На практике для увеличения времени перебора зачастую вводят сложный алгоритм генерации ключа (то есть пароль не применяется напрямую в качестве ключа для шифрования, его используют в качестве входных данных для некоего ресурсоемкого алгоритма, а на выходе получают ключ, как правило, фиксированной длины). В зависимости от конкретной системы, имеет смысл применять пароли длиной от 8 до 20 символов.

Примеры хороших паролей:

```
000hSADNARAk              SHE%as#$T^hoooo     CAM0BAP=X0POIIIO
YaLoveLapschu!SKuroy!     Xx.Pol13Potolok.xX  GHBdtnHT,znf!
```

Примеры плохих паролей:

```
   123456q ; 123321123321123321 ; qwerty ; Password ; 111111 ; qazwsx ;
abc123 ; rockyou  ; monkey ; iloveyou ; LOVELY  ; liverpool  ; tigger ;
pokemon ; Gfhjkm ; scooter ; newpw1; 121212 ; eatmyshirts ; q1w2e3 ;
qwe123 ; [duckitall] ; iphone5s ;
```

В случае, если приходится использовать множество паролей, возможно применение менеджера паролей. В этом случае потребуется запомнить только один сложный пароль.

2.2.2. Вредоносное ПО

Вредоносные программы. Понятие “вредоносные программы” (malware) объединяет все программы, создаваемые и используемые для осуществления несанкционированных и зачастую вредоносных действий. Вирусы, backdoor-программы (создаваемые для незаконного удаленного администрирования), клавиатурные шпионы, программы для кражи паролей, для блокирования файлов или компьютера, макровирусы для Word и Excel, вирусы сектора загрузки, скриптовые вирусы (BAT-вирусы, windows shell-вирусы, java-вирусы и т.д.) и скриптовые троянцы, мошенническое ПО, шпионские и рекламные программы – это далеко неполный список того, что классифицируется как вредоносные программы.

Когда-то для описания всех вредоносных программ хватало понятий “вирус” и “троянец”. Однако технологии и методы заражения компьютеров с тех пор ушли вперед, и этих двух понятий стало недостаточно для описания всего существующего многообразия вредоносных программ.

Вирус – это саморазмножающаяся программа: она распространяется с файла на файл и с компьютера на компьютер. Кроме того, вирус может быть запрограммирован на уничтожение или повреждение данных.

Черви считаются подклассом вирусов, но обладают характерными особенностями. Червь размножается (воспроизводит себя), не заражая другие файлы. Он внедряется один раз на конкретный компьютер и ищет способы распространиться далее на другие компьютеры.

Вирус заражает тем большее количество файлов, чем дольше он находится на компьютере необнаруженным. Червь создает единственную копию своего кода. В отличие от вируса, код червя самостоятелен.

Другими словами, червь – это отдельный файл, в то время как вирус – это код, который внедряется в существующие файлы.

Троянская программа. В античной мифологии Троянский конь – это деревянная конструкция соответствующей формы, внутри которой греки проникли в Трою и таким образом смогли покорить и разрушить город. По классическому определению, троянец – это программа, которая внешне выглядит как легальный программный продукт, но при запуске совершает вредоносные действия. Троянские программы не могут распространяться сами по себе, и этим они отличаются от вирусов и червей.

Обычно троянцы скрытно устанавливаются на компьютер и выполняют вредоносные действия без ведома пользователя. Трояны разных видов составляют большую часть современных вредоносных программ; все они пишутся специально для выполнения конкретной зловредной функции. Чаще всего встречаются backdoor-троянцы (утилиты удаленного администрирования, часто включают в себя клавиатурные шпионы), троянцы-шпионы, троянцы для кражи паролей и троянцы-прокси, превращающие компьютер в машину для рассылки спама.

При drive-by загрузке, компьютер заражается при посещении веб-сайта, содержащего вредоносный код. Кибермошенники ищут в Интернете веб-серверы, уязвимые для взлома, чтобы вписать вредоносный код на веб-страницы (часто в виде вредоносного скрипта). Если в операционной системе или на приложениях не установлены обновления безопасности, то при посещении зараженного веб-сайта вредоносный код загружается на ваш компьютер автоматически.

Клавиатурный шпион – это программа, отслеживающая нажатия кнопок на клавиатуре. При помощи нее злоумышленник может получить доступ к конфиденциальным данным (логины, пароли, номера кредитных карт, PIN-коды и т.п.) Клавиатурные шпионы часто входят в состав backdoor-троянцев.

Руткит (rootkit) – это набор программ, используемый взломщиками чтобы скрыть свои действия от защитных решений. Термин пришел из Unix-систем и обозначает методы, которые авторы троянских программ, работающих под Windows, используют для маскировки вредоносной активности своих зловредов. Установленные в системе руткиты не только не видны пользователям, но и избегают обнаружения антивирусным ПО. Для этого руткит под видом легитимного драйвера интегрируется с ядром ОС, перехватывает вызовы системных функций

от приложений и модифицирует результаты их выполнения, удаляя упоминания файлов и процессов, связанных со своей активностью.

Рекламная программа. Понятие “adware” включает в себя программы, запускающие рекламу (часто в виде всплывающих окон) или перенаправляющие поисковые запросы на рекламные веб-сайты. Рекламное ПО часто бывает встроено в бесплатные или условно-бесплатные программы и устанавливается на компьютер пользователя одновременно с основным приложением без ведома и согласия пользователя. В некоторых случаях рекламное ПО может тайно загрузить и установить на ваш компьютер троянская программа.

Устаревшие, не обновленные вовремя версии веб-браузеров могут быть уязвимыми для хакерских инструментов, скачивающих рекламные программы на ваш компьютер. Существуют также «программы-угонщики браузеров», способные менять настройки интернет-обозревателей, переадресовывать неправильно набранные или неполные URL-адреса на конкретные веб-сайты или менять заданную вами домашнюю страницу. Они также могут перенаправлять поисковые запросы на платные (часто порнографические) веб-сайты.

Рекламные программы, как правило, никак не проявляют себя в системе: их не видно в списке программ на вкладке Пуск -> Программы, нет соответствующих иконок в области уведомлений системы и в списке задач. Для них редко предусмотрена процедура деинсталляции (удаления); попытка удалить их вручную может привести к неполадкам в работе программы-носителя (в составе которой была установлена рекламная программа).

Шпионские программы. Как следует из названия, эти программы предназначены для сбора данных и отправки их третьей стороне без согласия пользователя. Такие программы могут отслеживать нажатия клавиш (клавиатурные шпионы), собирать конфиденциальную информацию (пароли, номера кредитных карт, PIN-коды и т.д.), отслеживать адреса электронной почты в почтовом ящике или особенности работы в Интернете.

Ботнеты (или так называемые зомби-сети) создаются троянцами или другими специальными вредоносными программами (как правило, применяются руткиты) и централизованно управляются хозяином, который получает доступ к ресурсам всех зараженных компьютеров и использует их в своих интересах.

Фишинговая программа. Фишинг – это особый вид кибермошенничества, направленный на то, чтобы обманным путем заставить вас раскрыть персональные данные, как правило финансового характера. Мошенники создают поддельный веб-сайт, который выглядит как сайт банка (или как любой другой сайт, через который производятся финансовые операции, например eBay). Затем преступники пытаются завлечь вас на этот сайт, чтобы вы ввели на нем конфиденциальные данные, такие как логин, пароль или PIN-код. Зачастую вредоносные программы перенаправляют запросы пользователя на фишинговые страницы.

Признаки присутствия ВПО в системе. Перечислить все характерные признаки заражения сложно, потому что одни и те же симптомы могут быть вызваны как воздействием вредоносного ПО, так и иными программными или аппаратными проблемами. Вот лишь несколько примеров:

- Время загрузки компьютера или его производительность изменились без видимых причин.
- Системные звуки, воспроизводимые в случайном порядке.
- Неожиданный запуск программ (иногда можно заметить появление консольных приложений).
- Сетевой экран сообщает, что неизвестное приложение пытается соединиться с интернетом.
- Абоненты из адресной книги получают по электронной почте нежелательные сообщения.
- Системные сообщения об ошибках, нехарактерные для рассматриваемой системы.
- При включении компьютера операционная система не загружается.
- Пропажа или изменение файлов или папок.
- Загорается индикатор доступа к жесткому диску, хотя не выполняется программ, которые могли бы к нему обращаться.
- Неполадки при работе с интернетом – переадресация на фишинговые страницы, недоступность загрузки антивирусов, передача данных по сети при отсутствии разрешенной сетевой активности.

2.2.3. Как распространяется вредоносное ПО?

Вредоносные программы могут заражать другие компьютеры, используя целый ряд методов. В данном разделе рассмотрено несколько типичных механизмов передачи, используемых подобными программами.

Съемные носители. Первым и, по всей видимости, наиболее эффективным средством передачи компьютерных вирусов и других вредоносных программ (по крайней мере, до недавнего времени) являлась передача в составе файлов. При этом сначала файлы переносились на дискетах, затем стали передаваться по сети, а в настоящее время для этого используются устройства с интерфейсом USB и Firewire. Хотя скорость распространения вредоносных программ при использовании данного механизма не столь высока, как при распространении по сети, опасность заражения сохраняется и от нее невозможно полностью защититься в силу необходимости обмена данными между системами.

Веб-сайты. Многие начинающие пользователи при поиске информации в интернете могут загрузить вредоносную программу под видом запрашиваемого файла. Кроме того, некоторые сайты могут использовать уязвимости, чтобы атаковать компьютеры посетителей.

Общие сетевые диски. Как только у компьютеров появилась возможность напрямую подключаться друг к другу по сети, разработчики вредоносных программ получили в свое распоряжение еще один механизм распространения вредоносного кода, возможности которого намного превосходят возможности использования съемных носителей. Низкий уровень безопасности общих сетевых дисков приводит к тому, что вредоносные программы могут заражать большое число подключенных к сети компьютеров. В результате этот метод распространения стал использоваться намного шире, чем передача вредоносного кода с помощью съемных носителей

Сканирование сети. Разработчики вредоносных программ используют данный механизм для поиска уязвимых компьютеров или атаки на случайные IP-адреса. Например, при использовании данного механизма может отправляться в конкретный порт некоторого диапазона IP-адресов специальный пакет, использующий определенную уязвимость, чтобы найти компьютеры, уязвимые для соответствующей атаки.

Одноранговые сети. Чтобы передавать файлы с помощью одноранговых сетей, на компьютере необходимо предварительно установить клиентский компонент соответствующего приложения для работы с одноранговыми сетями, который будет использовать один из сетевых портов, разрешенных в конфигурации корпоративного межсетевого экрана (например, порт 80). Клиентское приложение использует этот порт для передачи пакетов через межсетевой экран и обмена фай-

лами между компьютерами напрямую. Подобные приложения широко доступны в Интернете и предоставляют механизм передачи, помогающий разработчикам вредоносных программ передавать зараженные файлы на компьютеры пользователей.

Электронная почта. Данный механизм распространения используется многими вредоносными программами и является чрезвычайно эффективным, поскольку электронная почта позволяет разработчику вредоносной программы передавать вредоносный код сотням тысяч людей, не отходя от компьютера, а методы социальной инженерии дают возможность достаточно легко обмануть пользователя, заставив его открыть вложенные в сообщение файлы. Поэтому многие наиболее распространенные вредоносные программы используют для передачи своего кода на новые компьютеры именно этот метод. Существует два основных типа вредоносных программ, распространяющихся по электронной почте.

- Программа рассылки. Вредоносные программы данного типа отправляют себя по ограниченному числу адресов электронной почты с помощью установленных на компьютере средств работы с электронной почтой (например, Microsoft Outlook® Express) или с помощью собственных средств работы с протоколом SMTP.•
- Программа массовой рассылки. Вредоносные программы данного типа находят хранящиеся на зараженном компьютере адреса электронной почты и отправляют себя по всем найденным адресам с помощью установленных на компьютере средств работы с электронной почтой или с помощью собственных средств работы с протоколом SMTP.

Использование уязвимости удаленного доступа. Вредоносные программы могут использовать для своего распространения уязвимости в службах и приложениях. Такое поведение характерно для программ-червей. Например, программа-червь Slammer использовала уязвимость в Microsoft SQL Server™ 2000, вызывая переполнение буфера, позволяющее сохранять в системной памяти код, который мог выполняться в контексте безопасности службы SQL Server. Переполнением буфера называется состояние, которое возникает при занесении в буфер больше данных, чем это предусмотрено разработчиком. Злоумышленник может использовать эту уязвимость, чтобы получить полный доступ к компьютеру. Корпорация Майкрософт обнаружила и устранила данную уязвимость за несколько месяцев до появления червя Slammer, однако лишь немногие пользователи установили соответ-

ствующее обновление, в результате чего программа-червь смогла широко распространиться.

2.3. Защита операционных систем семейства Windows

В наше время обеспечение безопасности является неотъемлемой частью работы как для системных администраторов в крупных и даже мелких предприятиях, так и для домашних пользователей, перед которыми стоит задача настройки компьютера. Неопытные администраторы и домашние пользователи могут посчитать, что после установки антивируса и брандмауэра их операционные системы надежно защищены, но это не совсем так. Конечно, эти компьютеры будут защищены от множества атак, но что же спасет их от человеческого фактора? Сейчас возможности операционных систем по обеспечению безопасности очень велики. Существуют тысячи параметров безопасности, которые обеспечивают работу служб, сетевую безопасность, ограничение доступа к определенным ключам и параметрам системного реестра, управление агентами восстановления данных шифрования дисков BitLocker, управление доступом к приложениям и многое, многое другое.

В связи с широким распространением операционных систем Windows Server 2008 R2 и Windows 7, в этом разделе будут подробно описаны действия, необходимые для редактирования локальной политики безопасности в этих системах.

2.3.1. Контроль учётных записей (User Account Control)

Большинство проблем, связанных с безопасностью в последних версиях Windows были вызваны одной главной причиной: большинство пользователей запускали Windows, обладая правами администратора. Администраторы могут делать все что угодно с компьютером, работающим под управлением Windows: инсталлировать программы, добавлять устройства, обновлять драйвера, инсталлировать обновления, изменять параметры реестра, запускать служебные программы, а также создавать и модифицировать учетные записи пользователей. Несмотря на то, что это очень удобно, наличие этих прав приводит к возникновению огромной проблемы: любая шпионская программа, внедрившаяся в систему, тоже сможет работать, имея права администратора, и, таким образом, может нанести огромный урон, как самому компьютеру, так и всему, что к нему подключено.

В Windows XP эту проблему пытались решить путем создания второго уровня учетных записей, называемых **ограниченными пользователями**, которые обладали только самыми необходимыми разрешениями, но имели ряд недостатков. В Windows Vista снова попытались устранить эту проблему. Это решение называется «**Контроль учетных записей пользователей**», в основе которого был заложен принцип **наименее привилегированного пользователя**. Идея заключается в том, чтобы создать уровень учетной записи, который бы имел прав не больше, чем ему требовалось. Под такими учетными записями невозможно вносить изменения в реестр и выполнять другие административные задачи. Контроль учетных записей используется для уведомления пользователя перед внесением изменений, требующих прав администратора. С появлением UAC модель управления доступом изменилась таким образом, чтобы можно было помочь смягчить последствия вносимые вредоносными программами. Когда пользователь пытается запустить определенные компоненты системы или службы, появляется диалог контроля учетными записями, который дает пользователю право выбора: продолжать ли действие для получения административных привилегий или нет. Если пользователь не обладает правами администратора, то он должен в соответствующем диалоге предоставить данные учетной записи администратора для запуска необходимой ему программы. Для применения установок UAC требует только одобрение администратора, в связи с этим несанкционированные приложения не смогут устанавливаться без явного согласия администратора.

По сравнению с Windows Vista и Windows Server 2008 в операционных системах Windows 7 и Windows Server 2008 R2 появились следующие улучшения в функционале контроля учетных записей пользователей:

- Увеличилось количество задач, которые может выполнять обычный пользователь без запроса подтверждения администратором;
- Пользователю с правами администратора разрешается настраивать уровень UAC из «Панели Управления»;
- Существуют дополнительные настройки локальной политики безопасности, которые позволяют локальным администраторам изменять поведение сообщений UAC для локальных администраторов в режиме одобрения администратором;

• Существуют дополнительные настройки локальной политики безопасности, которые позволяют локальным администраторам изменять поведение сообщений UAC для обычных пользователей.

Большинству пользователей не нужен высокий уровень доступа к компьютеру и операционной системе. Чаще всего пользователи не подозревают, что они вошли в систему как администраторы, когда они проверяют электронную почту, занимаются веб-серфингом или запускают программное обеспечение. Вредоносная программа, установленная администратором, может повредить систему и воздействовать на всех пользователей. В связи с тем, что UAC требует одобрение администратором применение установки, несанкционированные приложения не смогут быть установленными автоматически без явного согласия администратором системы.

В связи с тем, что UAC позволяет пользователям запускать приложения как обычные пользователи:

• ИТ-отделы могут быть уверены в целостности их окружающей среды, включая системные файлы, журналы аудита, а также настройки системы;

• Администраторам больше не приходится тратить много времени на определение разрешений для задач на отдельных компьютерах;

• Администраторам предоставляется более эффективный контроль над лицензированием программного обеспечения, поскольку они могут обеспечить установку только авторизованных приложений. Им больше не придется беспокоиться о возможных угрозах их сетей из-за нелицензионного или вредоносного программного обеспечения.

Спецификации UAC

Маркер доступа. Маркеры доступа содержат информацию безопасности сеанса входа, определяющую пользователя, группы пользователей и привилегии. Операционная система использует маркер доступа для контроля доступа к защищаемым объектам и контролирует возможность выполнения пользователем различных связанных с системой операций на локальном компьютере. Маркеры доступа UAC – это особый вид маркеров доступа, определяющих минимальные привилегии, необходимые для работы – привилегии интерактивного доступа по умолчанию для пользователя Windows в системе с включенной функцией UAC. Второй маркер, маркер полного доступа админи-

стратора, имеет максимальные привилегии, разрешенные для учетной записи администратора. Когда пользователь входит в систему, то для этого пользователя создается маркер доступа. Маркер доступа содержит информацию об уровне доступа, который выдается пользователю, в том числе идентификаторы безопасности (SID).

Режим одобрения администратором. Режим одобрения администратором – это конфигурация управления учетными записями пользователей, в которой для администратора создается пользовательский маркер комбинированного доступа. Когда администратор входит в компьютер с ОС Windows, ему назначаются два отдельных маркера доступа. Если режим одобрения администратором не используется, администратор получает только один маркер доступа, предоставляющий ему доступ ко всем ресурсам Windows.

Запрос согласия. Запрос согласия отображается в том случае, когда пользователь пытается выполнить задачу, которая требует права администратора. Пользователь дает согласие или отказывается, нажимая на кнопку «Да» или «Нет».

Запрос учетных данных. Запрос учетных данных отображается для обычных пользователей в том случае, когда они пытаются выполнить задачу, для которой необходим доступ администратора. Пользователь должен указать имя и пароль учетной записи, которая входит в группу локальных администраторов.

Принцип работы UAC

Контроль учетных записей пользователей (UAC) помогает предотвращать заражение компьютера от вредоносных программ, помогая организациям более эффективно разворачивать настольные приложения.

С использованием UAC, приложения и задачи всегда запускаются в безопасной области от неадминистраторской учетной записи, если администратор дает права для административного доступа в системе.

Панель управления UAC позволяет выбрать один из четырех вариантов:

1. Уведомлять при каждом изменении, вносимом в систему: такое поведение присутствует в Vista – диалог UAC появляется каждый раз, когда пользователь пытается внести любое изменение в систему (настройка Windows, установка приложений и т.д.)

2. *Уведомлять только тогда, когда приложения пытаются внести изменения в систему*: в этом случае уведомление не появится при внесении изменений в Windows, например, через панель управления и оснастки.

3. *Уведомлять только тогда, когда приложения пытаются внести изменения в систему, без использования безопасного рабочего стола*: то же самое, что и пункт 2, за исключением того, что диалог UAC появляется в виде традиционного диалога, а не в режиме безопасного рабочего стола. Несмотря на то, что это может оказаться удобным в случае использования определенных графических драйверов, затрудняющих переключение между рабочими столами, этот режим является барьером на пути приложений, имитирующих поведение UAC.

4. *Никогда не уведомлять*: данная настройка полностью отключает UAC.

Процессы и взаимодействия UAC

Для обеспечения безопасности, по умолчанию, доступ к системным ресурсам и приложениям, обычным пользователям и администраторам предоставляется в режиме обычного пользователя. Когда пользователь входит в систему, то для него создается маркер доступа. Маркер доступа содержит информацию об уровне доступа, который задается пользователю, в том числе и идентификаторы безопасности (SID).

Когда администратор входит в систему, создается два отдельных пользовательских маркера: маркер доступа стандартного пользователя и маркер полного доступа администратора. В стандартном пользовательском доступе содержится та же пользовательская информация, что и в маркере полного доступа администратора, но без административных привилегий и SID. Маркер доступа стандартного пользователя используется для запуска приложений, которые не выполняют административные задачи. Доступ стандартного пользователя используется только для отображения рабочего стола (explorer.exe). Explorer.exe является родительским процессом, из-под которого пользователь может запускать другие процессы, наследуемые своим маркером доступа. В результате все приложения запускаются от имени обычного пользователя, кроме тех случаев, когда приложения требует использования административного доступа.

Пользователь, который является членом группы «Администраторы» может войти в систему для просмотра веб-страниц и чтения сообщений электронной почты при использовании стандартного маркера

пользовательского доступа. Когда администратору необходимо выполнить задачу, которая требует от него маркер административного пользователя, Windows 7 автоматически покажет уведомление для использования административных прав. Это уведомление называется запросом учетных данных, а его поведение может быть настроено при помощи оснастки локальной политики безопасности (Secpol.msc) или групповых политик.

Каждое приложение, которое требует маркер доступа администратора должно запускаться с согласием администратора. Исключением является взаимосвязь между родительским и дочерним процессами. Дочерние процессы наследуют маркер доступа пользователей из родительского процесса. Оба процесса родителя и ребенка должны иметь одинаковый уровень интеграции.

Windows 7 защищает процессы при помощи маркировки уровней интеграции. Уровни интеграции измеряются доверием. Приложения с «высокой» интеграцией – это приложения, выполняющие задачи, которые могут изменять системные данные. А приложения с «низкой» интеграцией – это выполняемые задачи, которые потенциально могут нанести ущерб операционной системе. Приложения с более низким уровнем интеграции не могут изменять данные в приложениях с высоким уровнем интеграции.

Когда обычный пользователь пытается запустить приложение, которое требует маркер доступа администратора, UAC требует пользователя предоставить данные администратора.

Пользовательские возможности UAC

При включенном UAC, пользовательские возможности отличаются от возможностей администратора в режиме одобрения администратором. Существует еще более безопасный метод входа в систему Windows 7 – создание основной учетной записи с правами обычного пользователя. Работа в качестве обычного пользователя позволяет максимально повысить степень безопасности. Благодаря встроенному в UAC компоненту полномочий обычные пользователи могут легко выполнять административные задачи путем ввода данных локальной учетной записи администратора.

Альтернативный вариант запуска приложений обычным пользователем является запуск приложений с повышенными правами администратора. С помощью встроенного в UAC компонента учетных данных, члены локальной группы Администраторы могут легко выпол-

нять административные задачи путем предоставления утверждающих данных. По умолчанию, встроенный компонент учетных данных для учетной записи администратора в режиме одобрения называется запросом согласий. *Запрос учетных данных UAC может быть настроен при помощи оснастки локальной политики безопасности (Secpol.msc) или групповых политик.*

Запросы согласия и учетных данных

С включенным UAC, Windows 7 запрашивает согласие или учетные данные записи локального администратора, перед запуском программы или задания, которое требует маркер полного доступа администратора. *Этот запрос не гарантирует того, что шпионские программы не могут быть установлены в тихом режиме.*

Запрос согласия

Запрос согласия отображается в том случае, когда пользователь пытается выполнить задачу, которая требует маркер доступа администратора.

Запрос учетных данных

Запрос учетных данных отображается в том случае, когда обычный пользователь пытается запустить задачу, которая требует маркер доступа администратора. Этот запрос для обычного пользователя может быть настроен при помощи оснастки локальной политики безопасности (Secpol.msc) или групповых политик. Запрос учетных данных также может быть настроен для администраторов при помощи изменения политики Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором со значением Запрос учетных данных.

Запросы на повышение прав UAC

Запросы на повышение прав UAC имеют цветовую маркировку для конкретных приложений, позволяя немедленно идентифицировать потенциальный риск безопасности. Когда приложение пытается запуститься с маркером полного доступа администратора, Windows 7 сначала анализирует исполняемый файл для определения издателя. Прежде всего, приложения делятся на 3 категории издателей исполняемого файла: Windows 7, проверенный издатель (подписанный), не проверенный издатель (не подписанный). На следующем изображении отображается то, как Windows 7 определяет какой цвет запроса повышения отображать пользователю.

Цветовая маркировка запросов на повышение прав следующая:

- На красном фоне отображен значок щита: приложение блокируется при помощи групповой политики или блокируется из-за неизвестного издателя.

- На синем фоне отображен золотистый значок щита: приложение является административным приложением Windows 7, таким как «Панель управления».

- На голубом фоне отображается синий значок щита: приложение подписано и является доверенным на локальном компьютере.

- На желтом фоне отображается желтый значок щита: приложение не подписано или подписано, но не является доверенным на локальном компьютере.

Значок щита

Некоторые элементы «Панели управления», такие как «Дата и время» содержат комбинацию операций администратора и обычных пользователей. Обычные пользователи могут видеть время и изменять часовой пояс, маркер полного доступа администратора требуется для изменения даты и времени системы.

Значок щита на кнопке «Изменить дату и время» указывает на то, что этот процесс требует маркер полного доступа администратора и отобразит запрос на повышения прав UAC.

Обеспечение запроса на повышение прав

Процесс повышения прав обеспечивает прямые запросы для защиты рабочего стола. Запросы согласия и учетных данных отображаются по умолчанию в Windows 7 для обеспечения безопасности системы. Только системные процессы могут получить полный доступ к безопасной рабочей среде. Для достижения более высокого уровня безопасности рекомендуется включить групповую политику Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав.

Когда исполняемые файлы просят повышения прав, интерактивный рабочий стол, называемый также рабочим столом, переключается на безопасный рабочий стол. Безопасный рабочий стол затемняет пользовательский и отображает запрос на повышение прав, в котором пользователь должен принять решение для продолжения выполнения задачи. Когда пользователь нажимает на кнопку «Да» или«Нет», рабочий стол снова переключается на пользовательский.

Вредоносное программное обеспечение может имитировать безопасный рабочий стол, но при включенной политике «*Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором*» со значением «*Запрос согласия*» вредоносная программа не сможет получить повышенные права, если даже пользователь нажмет на кнопку «Да». Если параметр политики имеет значение «Запрос учетных данных», то вредоносное программное обеспечение, имитирующее безопасный рабочий стол, сможет собирать учетные данные пользователей.

Таким образом, контроль учетных записей призван не предотвратить проникновение вредоносного кода (для этого есть брандмауэр и антивирусное/антишпионское ПО), а снизить наносимый им ущерб – ограничить его влияние правами обычного пользователя. Строго говоря, повышается не безопасность операционной системы, а ее устойчивость к несанкционированному доступу.

2.3.2. Работа с учётными записями

Учётная запись пользователя – это запись, которая содержит сведения, необходимые для идентификации пользователя при подключении к системе, а также информацию для авторизации и учёта. Это имя пользователя и пароль (или другое аналогичное средство аутентификации – например, биометрические характеристики). Пароль или его аналог, как правило, хранится в зашифрованном или хэшированном виде (в целях его безопасности).

Для повышения надёжности могут быть, наряду с паролем, предусмотрены альтернативные средства аутентификации – например, специальный секретный вопрос (или несколько вопросов) такого содержания, что ответ может быть известен только пользователю. Такие вопросы и ответы также хранятся в учётной записи.

Учётная запись может содержать следующие дополнительные анкетные данные о пользователе:

- имя;
- фамилию;
- отчество;
- псевдоним (ник);
- пол;
- национальность;
- расовую принадлежность;
- вероисповедание
- группу крови;

- резус-фактор;
- возраст;
- дату рождения;
- адрес электронной почты;
- домашний адрес;
- рабочий адрес;
- нетмейловый адрес;
- номер домашнего телефона;
- номер рабочего телефона;
- номер мобильного телефона;
- номер ICQ;
- идентификатор Skype, ник в IRC;
- другие контактные данные систем обмена мгновенными сообщениями;
- адрес домашней страницы и/или блога в Интернете или интранете;
- сведения о хобби;
- сведения о круге интересов;
- сведения о семье;
- сведения о перенесённых болезнях;
- сведения о политических предпочтениях;
- и многое другое

Конкретные категории данных, которые могут быть внесены в такую анкету, определяются администраторами системы.

Учётная запись может также содержать одну или несколько фотографий или аватар пользователя. Учётная запись пользователя также может учитывать различные статистические характеристики поведения пользователя в системе: давность последнего входа в систему, продолжительность последнего пребывания в системе, адрес использованного при подключении компьютера, интенсивность использования системы, суммарное и (или) удельное количество определённых операций, произведённых в системе, и так далее.

Создание учетных записей пользователей

В операционной системе Windows 7 можно создавать несколькими способами как учетные записи пользователей для компьютеров, состоящих в рабочих группах, так и учетные записи пользователей для компьютеров, которые входят в состав домена. Домены, рабочие группы и домашние группы представляют разные методы организации

компьютеров в сети. Основное их различие состоит в том, как осуществляется управление компьютерами и другими ресурсами.

Рабочая группа – это группа компьютеров, подключенных к сети, которые совместно используют ресурсы. При настройке сети операционная система Windows автоматически создает рабочую группу и присваивает ей имя по умолчанию.

Домен – это группа компьютеров одной сети, имеющих единый центр, использующий единую базу пользователей, единую групповую и локальную политики, единые параметры безопасности, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров.

Создание учетных записей пользователей для компьютеров, состоящих в рабочей группе

В операционной системе Windows 7 для компьютеров, которые состоят в рабочей или домашней группе, учетные записи можно создавать следующими способами:

Создание учетной записи при помощи диалога «Управление учетными записями пользователей»

Для того чтобы создать учетную запись при помощи диалога «Учетные записи пользователей», нужно сделать следующее:

1. Нажмите на кнопку **«Пуск»** для открытия меню, откройте **«Панель управления»** и из списка компонентов панели управления выберите **«Учетные записи пользователей»**;
2. В диалоге **«Учетные записи пользователей»** перейдите по ссылке **«Управление другой учетной записью»**, а затем нажмите на **«Создание учетной записью»**;
3. Здесь нужно будет ввести имя для учетной записи, выбрать тип учетной записи и нажать на кнопку **«Создание учетной записи»**;

Имя пользователя не должно совпадать с любым другим именем пользователя или группы на данном компьютере. Оно может содержать до 20 символов верхнего или нижнего регистров, за исключением следующих: « / \ [ ] : ; | = , + * ? <> @, а также имя пользователя не может состоять только из точек и пробелов.

В этом диалоге, можно выбрать одну из двух типов учетных записей: **«обычные учетные записи пользователей»**, которые предназна-

чены для повседневной работы или **«учетные записи администратора»**, которые предоставляют полный контроль над компьютером и применяются только в необходимых случаях.

Создание учетной записи при помощи диалога «Учетные записи пользователей»

Доступный через панель управления диалог «Управление учетными записями пользователей» имеет очень серьезное ограничение: оно предлагает на выбор только учетные записи типа *Обычный доступ* или *Администратор*. Для того чтобы при создании нового пользователя его можно было поместить в какую-либо определенную группу, нужно сделать следующее:

1. Воспользоваться комбинацией клавиш +R для открытия диалога **«Выполнить»**;
2. В диалоговом окне **«Выполнить»**, в поле **«Открыть»** введите *control userpasswords2* и нажмите на кнопку **«ОК»**;
3. В диалоговом окне **«Учетные записи пользователей»** нажмите на кнопку **«Добавить»** для запуска мастера добавления нового пользователя;
4. В появившемся диалоговом окне **«Добавление нового пользователя»** введите имя пользователя. Поля **«Полное имя»** и **«Описание»** не являются обязательными, то есть их можно заполнять при желании. Нажимаем на кнопку **«Далее»**;
5. В диалоге **«Введите и подтвердите пароль этого пользователя»** введите пароль для данной учетной записи, а затем продублируйте его в поле **«Подтверждение»**, после чего нажмите на кнопку **«Далее»**;
6. Это последний диалог мастера добавления нового пользователя. Здесь необходимо установить переключатель, определяющий группу безопасности, к которой должна относиться данная учетная запись пользователя. Можно выбрать одну из следующих групп: Обычный доступ, Администратор или Другой. Последний переключатель стоит использовать в том случае, если нужно отнести пользователя к какой-то другой группе, созданной по умолчанию в операционной системе Windows 7.

В следующем списке перечислены 15 встроенных групп операционной системы Windows 7. Эти права назначаются в рамках локальных политик безопасности:

- **Administrators (Администраторы)**. Пользователи, входящие в эту группу, имеют полный доступ на управление компьютером и могут при необходимости назначать пользователям права пользователей и разрешения на управление доступом. По умолчанию членом этой группы является учетная запись администратора. Если компьютер подключен к домену, группа **«Администраторы домена»** автоматически добавляется в группу **«Администраторы»**. Эта группа имеет полный доступ к управлению компьютером, поэтому необходимо проявлять осторожность при добавлении пользователей в данную группу;
- **Backup Operators (Операторы архива)**. Пользователи, входящие в эту группу, могут архивировать и восстанавливать файлы на компьютере независимо от любых разрешений, которыми защищены эти файлы. Это обусловлено тем, что право выполнения архивации получает приоритет над всеми разрешениями. Члены этой группы не могут изменять параметры безопасности.
- **Cryptographic Operators (Операторы криптографии)**. Членам этой группы разрешено выполнение операций криптографии.
- **Debugger Users (Группа удаленных помощников)**. Члены этой группы могут предлагать удаленную помощь пользователям данного компьютера.
- **Distributed COM Users (Пользователи DCOM)**. Членам этой группы разрешено запускать, активировать и использовать объекты DCOM на компьютере.
- **Event Log Readers (Читатели журнала событий)**. Членам этой группы разрешается запускать журнал событий Windows.
- **Guests (Гости)**. Пользователи, входящие в эту группу, получают временный профиль, который создается при входе пользователя в систему и удаляется при выходе из нее. Учетная запись**«Гость»** (отключенная по умолчанию) также является членом данной встроенной группы.
- **IIS_IUSRS**. Это встроенная группа, используемая службами IIS.
- **Network Configuration Operators (Операторы настройки сети)**. Пользователи, входящие в эту группу, могут изменять параметры TCP/IP, а также обновлять и освобождать адреса TCP/IP. Эта группа не имеет членов по умолчанию.
- **Performance Log Users (Пользователи журналов производительности)**. Пользователи, входящие в эту группу, могут управлять счетчиками производительности, журналами и оповеще-

ниями на локальном или удаленном компьютере, не являясь при этом членами группы **«Администраторы»**.

- **Performance Monitor Users (Пользователи системного монитора)**. Пользователи, входящие в эту группу, могут наблюдать за счетчиками производительности на локальном или удаленном компьютере, не являясь при этом участниками групп **«Администраторы»** или **«Пользователи журналов производительности»**.
- **Power Users (Опытные пользователи)**. По умолчанию, члены этой группы имеют те же права пользователя и разрешения, что и учетные записи обычных пользователей. В предыдущих версиях операционной системы Windows эта группа была создана для того, чтобы назначать пользователям особые административные права и разрешения для выполнения распространенных системных задач. В этой версии операционной системы Windows учетные записи обычных пользователей предусматривают возможность выполнения большинства типовых задач настройки, таких как смена часовых поясов. Для старых приложений, требующих тех же прав опытных пользователей, которые имелись в предыдущих версиях операционной системы Windows, администраторы могут применять шаблон безопасности, который позволяет группе **«Опытные пользователи»** присваивать эти права и разрешения, как это было в предыдущих версиях операционной системы Windows.
- **Remote Desktop Users (Пользователи удаленного рабочего стола)**. Пользователи, входящие в эту группу, имеют право удаленного входа на компьютер.
- **Replicator (Репликатор)**. Эта группа поддерживает функции репликации. Единственный член этой группы должен иметь учетную запись пользователя домена, которая используется для входа в систему службы репликации контроллера домена. Не добавляйте в эту группу учетные записи реальных пользователей.
- **Users (Пользователи)**. Пользователи, входящие в эту группу, могут выполнять типовые задачи, такие как запуск приложений, использование локальных и сетевых принтеров и блокировку компьютера. Члены этой группы не могут предоставлять общий доступ к папкам или создавать локальные принтеры. По умолчанию членами этой группы являются группы **«Пользователи домена»**, **«Проверенные пользователи»** и **«Интерак-**

тивные». Таким образом, любая учетная запись пользователя, созданная в домене, становится членом этой группы.

Создание учетной записи при помощи оснастки «Локальные пользователи и группы»

Оснастка «Локальные пользователи и группы» расположена в компоненте «Управление компьютером», представляющем собой набор средств администрирования, с помощью которых можно управлять одним компьютером, локальным или удаленным. Оснастка «Локальные пользователи и группы» служит для защиты и управления учетными записями пользователей и групп, размещенных локально на компьютере. Можно назначать разрешения и права для учетной записи локального пользователя или группы на определенном компьютере (и только на этом компьютере).

Использование оснастки **«Локальные пользователи и группы»** позволяет ограничить возможные действия пользователей и групп путем назначения им прав и разрешений. Право дает возможность пользователю выполнять на компьютере определенные действия, такие как архивирование файлов и папок или завершение работы компьютера. Разрешение представляет собой правило, связанное с объектом (обычно с файлом, папкой или принтером), которое определяет, каким пользователям, и какой доступ к объекту разрешен.

Для того чтобы создать локальную учетную запись пользователя при помощи оснастки **«Локальные пользователи и группы»**, нужно сделать следующее:

1. Откройте оснастку **«Локальные пользователи и группы»** одним из следующих способов:
   - Нажмите на кнопку **«Пуск»** для открытия меню, откройте **«Панель управления»** и из списка компонентов панели управления выберите **«Администрирование»**, затем откройте компонент **«Управление компьютером»**. В **«Управлении компьютером»** откройте **«Локальные пользователи и группы»**;
   - Открыть **«Консоль управления ММС»**. Для этого нажмите на кнопку **«Пуск»**, в поле поиска введите *mmc*, а затем нажмите на кнопку **«Enter»**. Откроется пустая консоль ММС. В меню**«Консоль»** выберите команду **«Добавить или удалить оснастку»** или воспользуйтесь комбинацией клавиш Ctrl+M. В диалоге **«Добавление и удаление оснасток»** выберите оснастку **«Локальные пользователи и группы»** и нажмите на кнопку

«Добавить». Затем нажмите на кнопку **«Готово»**, а после этого – кнопку **«ОК»**. В дереве консоли откройте узел**«Локальные пользователи и группы (локально)»**;

- Воспользоваться комбинацией клавиш +R для открытия диалога **«Выполнить»**. В диалоговом окне **«Выполнить»**, в поле **«Открыть»** введите *lusrmgr.msc* и нажмите на кнопку **«ОК»**;

2. Откройте узел **«Пользователи»** и либо в меню **«Действие»**, либо из контекстного меню выбрать команду **«Новый пользователь»**;
3. В диалоговом окне **«Новый пользователь»** введите соответствующие сведения. Помимо указанных данных, можно воспользоваться следующими флажками: **Требовать смену пароля при следующем входе в систему**, **Запретить смену пароля пользователем**, **Срок действия пароля не ограничен**, **Отключить учетную запись** и нажать на кнопку **«Создать»**, а затем **«Закрыть»**.

Для того чтобы добавить пользователя в группу, дважды щелкните имя пользователя для получения доступа к странице свойств пользователя. На вкладке **«Членство в группах»** нажмите на кнопку **«Добавить»**.

В диалоге **«Выбор группы»** можно выбрать группу для пользователя двумя способами:

1. В поле **«Введите имена выбираемых объектов»** введите имя группы и нажмите на кнопку **«Проверить имена»;**
2. В диалоге **«Выбор группы»** нажмите на кнопку **«Дополнительно»**, чтобы открыть диалоговое окно **«Выбор группы»**. В этом окне нажмите на кнопку **«Поиск»**, чтобы отобразить список всех доступных групп, выберите подходящую группу и нажмите два раза на кнопку «ОК».

Создание учетной записи при помощи командной строки

Помимо вышеперечисленных способов, учетные записи пользователей можно создавать, изменять и удалять при помощи командной строки. Для этого нужно выполнить следующие действия:

1. Запустите командную строку от имени администратора;
2. Для создания учетной записи при помощи командной строки используйте команду *net user*.

Команда net user используется для добавления пользователей, установки паролей, отключения учетных записей, установки параметров и удаления учетных записей. При выполнении команды без параметров командной строки отображается список учетных записей пользователей, присутствующих на компьютере. Информация об учетных записях пользователей хранится в базе данных учетных записей пользователей.

Пример команды:

```
   net user User /add /passwordreq:yes /times:Monday-Friday,9am-6pm
/fullname:"New user"
```

Используемые параметры:

/add – этот параметр указывает, что необходимо создать новую учетную запись;

/passwordreq – этот параметр отвечает за то, чтобы при первом входе в систему пользователь сменил свой пароль;

/times – этот параметр определяет, сколько раз пользователю разрешено входить в систему. Здесь можно указывать как единичные дни, так и целые диапазоны (например Sa или M-F). Для указания времени допускается как 24-часовый формат, так и 12-часовый формат;

/fullname – этот параметр идентичен полю «Полное имя» при создании пользователя предыдущими способами.

Создание учетных записей пользователей для компьютеров, состоящих в домене

В серверной операционной системе Windows Server 2008 или Windows Server 2008 R2 в домене Active Directory учетные записи пользователей можно создавать шестью способами. Рассмотрим подробно каждый из них:

Создание пользователей при помощи оснастки «Active Directory – пользователи и компьютеры»

Для создания нового пользователя в домене при помощи оснастки «Active Directory – пользователи и компьютеры» нужно сделать следующее:

1. Открыть оснастку **«Active Directory – пользователи и компьютеры»**;
2. В дереве консоли разверните узел, предоставляющий домен и найдите контейнер, в котором нужно создать учетную запись пользователя;

3. Нажмите на подразделение или контейнер правой кнопкой мыши, выберите опцию **«Создать»** и примените команду **«Пользователь»**;
4. В диалоговом окне **«Новый объект – пользователь»** введите в поле **«Имя»** - имя пользователя, в поле **«Инициалы»** - его инициалы, в поле **«Фамилия»** - фамилию пользователя. Поле**«Полное имя»** должно заполниться автоматически, согласно CN пользователя. В поле **«Имя входа»** введите имя входа пользователя в систему и в раскрывающемся списке выберите суффикс основного имени пользователя, который будет прикреплен к имени входа с символом @. В поле **«Имя входа пользователя (пред-Windows 2000)»** введите имя входа для систем, предшествующих Windows 2000, так называемое низкоуровневым именем входа. Нажать на кнопку **«Далее»**.
5. В следующем диалоге введите пароль для данной учетной записи, а затем продублируйте его в поле **«Подтверждение»** и установите нужные флажки, после чего нажмите на кнопку **«Далее»**.
6. В последнем диалоге можно просмотреть введенные параметры и нажать на кнопку **«Готово»** для создания нового пользователя.

Создание пользователей с помощью командной строки

Для автоматизации создания любых объектов в домене Active Directory можно использовать команду *DSADD USER UserDN*, при помощи которой можно создавать объекты пользователей и принимать параметры, указывающие его свойства. Нового пользователя при помощи командной строки можно создать следующим образом:

```
   dsadd user «CN=Дмитрий Буланов,OU=Кадры,DC=server,DC=com»
-samid Dmitry.bulanov –pwd * -mustchpwd yes
-profile \\server01\Profiles\dmitry.bulanov -fn «Дмитрий» -ln «Буланов»
-display «Дмитрий Буланов» –upn Dmitry.bulanov@server.com
```

Определение используемых параметров:

Samid – указывает имя входа пользователя;

Pwd – этот параметр определяет пароль для учетной записи пользователя. Если указывать символ *, то будет предложено ввести пароль пользователя;

Mustchpwd – указывает, что пользователь должен изменить свой пароль при следующем входе в систему;

Profile – указывает путь к профилю учетной записи пользователя;

Fn – указывает имя пользователя;

Ln – указывает фамилию пользователя;

Display – указывает отображаемое имя пользователя;

Upn – указывает имя входа пользователя (пред-Windows 2000).

Импорт пользователей с помощью команды CSVDE

Утилита командной строки CSVDE позволяет импортировать и экспортировать объекты Active Directory в виде текстового файла с разделенными запятыми (Comma-Separated Values, *.csv). Эти файлы можно создавать и изменять при помощи таких программ, как Блокнот или, например, Microsoft Office Excel. Эта утилита – способ автоматизации создания учетных записей пользователя на основе информации пользователей из базы данных Excel и Microsoft Office Access. Команда импортирует текстовый файл, в котором строка определяет атрибуты импорта с помощью их имен LDAP. Синтаксис команды следующий:

```
Csvde –i –f имя_файла –k
```

Параметр i указывает режим импорта, а параметр k используется для игнорирования ошибок.

CSV файл должен выглядеть следующим образом:

```
DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName
«cn=Дмитрий Буланов,ou=Пользователи,dc=server,dc=com»,user,
Dmitry.bulanov,Буланов,Дмитрий,42mitry.bulanov@server.com
```

Импортировать пароли при помощи команды CSVDE нельзя.

Импорт пользователей с помощью команды LDIFDE

При помощи команды LDIFDE также можно импортировать и экспортировать объекты Active Directory. В данном случае используется стандарт файлового формата LDIF (Lightweight Directory Access Protocol Data Interchange Format). Этот файловый формат состоит из блока строк, которые вместе образуют одну операцию. Разные операции разделяются пустой строкой. Каждая строка содержит имя атрибута, а после него должно стоять двоеточие со значением атрибута. Далее можно увидеть листинг LDIF файла:

```
DN: CN=Дмитрий Буланов, OU=пользователи, DC=server, DC=com
changeType: add
CN: Дмитрий Буланов
objectClass: user
sAMAccountName: Dmitry.bulanov
userPrincipalName: Dmitry.bulanov@server.com
givenName: Дмитрий
sn: Буланов
displayName: Дмитрий Буланов
```

Файл можно создавать в такой программе как Блокнот, но сохранять его нужно с расширением *.ldf. в командной строке введите следующее:

```
Ldifde –i –f имя_файла –k
```

Создание пользователей с помощью Windows PowerShell

При помощи Windows PowerShell для создания пользователя в Active Directory пользователя можно создать следующим образом:

1. Подключитесь к контейнеру, в котором будет создан объект;
2. Примените метод Create совместно с классом и отличительным именем RDN;
3. Заполните атрибуты при помощи метода Put;
4. Подтвердите изменения при помощи метода SetInfo.

Далее можно увидеть листинг скрипта PowerShell - *.ps1-файла:

```
$ObjOU=[ADSI]”LDAP://OU=Пользователи,DC=server,DC=com”
$ObjUser=$ObjOU.Create(“user”, “CN=Дмитрий Буланов”)
$ObjUser.Put(“sAMAccountName”, “43mitry.bulanov”)
$ObjUser.Put(“userPrincipalName”, “43mitry.bulanov @server.com”)
$ObjUser.Put(“displayName”, “Дмитрий Буланов”)
$ObjUser.Put(“givenName”, “Дмитрий”)
$ObjUser.Put(“sn”, “Буланов”)
$ObjUser.Put(«description», «Тестировщик программного обеспечения»)
$ObjUser.Put(“company”, “Company”)
$ObjUser.Put(“department”, “Отдел тестирования”)
$ObjUser.Put(«title», «Тестировщик программного обеспечения»)
$ObjUser.Put(“mail”, “ 43mitry.bulanov @server.com “)
$ObjUser.Put(“c”, “UA”)
$ObjUser.Put(“postalCode”, “73003”)
$ObjUser.Put(“st”, “Херсон”)
$ObjUser.Put(“l”, “Херсон”)
$ObjUser.Put(“streetAddress”, “Улица”)
$ObjUser.Put(“postOfficeBox”, “Номер дома”)
$ObjUser.SetInfo()
$ObjUser.SetPassword(“P@ssword”)
//$ObjUser.Put(«pwdLastSet», 0) – для смены пароля при следующем старте
$ObjUser.psbase.InvokeSet(“AccountDisabled”,$false)
$ObjUser.SetInfo()
```

Можно вводить все строки вручную, а можно использовать *.ps1-файлы для автоматизации создания новых пользователей. Для того, чтобы разрешить Windows PowerShell открывать скрипты, введите следующую команду:

```
Set-ExecutionPolicy RemoteSigned
```

Политика выполнения указывает сценарии, которые можно запускать. После назначения политики выполнения можно запустить сценарий, но если указывать для запуска только имя сценария, то может возникнуть ошибка. Чаще всего нужно будет указывать еще и путь к самому сценарию.

Создание пользователей с помощью VBScript

В связи с тем, что VBScript также как и Windows PowerShell использует интерфейс ADSI для манипулирования объектами в Active Directory, процесс создания пользователя в VBScript идентичен созданию пользователя в Windows PowerShell. Прежде всего, сценарий подключается к контейнеру OU, в котором будет создан пользователь. После чего сценарий применит к объекту ADSI инструкцию GetObject. При присвоении объекта переменной, для создания объектной ссылки используется инструкция Set.

После этого активизируется метод Create для создания объекта конкретного класса так же, как и в PowerShell. Далее используется метод Put, но аргументы заключаются в круглые скобки. Последняя строка – идентична Windows PowerShell. Пример скрипта:

```
Set objOU=GetObject(“LDAP: //OU=Пользователи,DC=server,DC=com”)
Set objUser=objOU.Create(“user”,”CN=Дмитрий Буланов”)
objUser.Put “sAMAccountName”,” 44mitry.bulanov”
objUser.Put “displayName”,” Дмитрий Буланов”
objUser.Put “givenName”,” Дмитрий”
objUser.Put “sn”,” Буланов”
ObjUser.SetInfo()
```

2.3.3. Конфигурирование политик безопасности

Политика безопасности – это набор параметров, которые регулируют безопасность компьютера и управляются с помощью локального объекта GPO. Настраивать данные политики можно при помощи оснастки **«Редактор локальной групповой политики»** или оснастки **«Локальная политика безопасности»**. Оснастка **«Локальная политика безопасности»** используется для изменения политики учетных

записей и локальной политики на локальном компьютере, а политики учетных записей, привязанных к домену Active Directory можно настраивать при помощи оснастки **«Редактор управления групповыми политиками»**. Перейти к локальным политикам безопасности, вы можете следующими способами:

В том случае, если ваш компьютер подсоединен к домену Active Directory, политика безопасности определяется политикой домена или политикой подразделения, членом которого является компьютер.

Применение политики безопасности для локального компьютера

Для успешного выполнения текущего примера, учетная запись, под которой выполняются данные действия, должна входить в группу **«Администраторы»** на локальном компьютере. Если компьютер подключен к домену, то эти действия могут выполнять только пользователи, которые являются членами группы **«Администраторы домена»** или групп, с разрешенными правами на редактирование политик.

В этом примере мы переименуем гостевую учетную запись. Для этого выполните следующие действия:

1. Откройте оснастку **«Локальные политики безопасности»** или перейдите в узел **«Параметры безопасности»** оснастки **«Редактор локальной групповой политики»**;
2. Перейдите в узел **«Локальные политики»**, а затем **«Параметры безопасности»**;
3. Откройте параметр **«Учетные записи: Переименование учетной записи гостя»** дважды щелкнув на нем или нажав на клавишу **Enter**;
4. В текстовом поле введите *Гостевая запись* и нажмите на кнопку **«ОК»**;
5. Перезагрузите компьютер.

После перезагрузки компьютера для того чтобы проверить, применилась ли политика безопасности к вашему компьютеру, вам нужно открыть в панели управления компонент **«Учетные записи пользователей»** и перейти по ссылке **«Управление другой учетной записью»**. В открывшемся окне вы увидите все учетные записи, созданные на ва-

шем локальном компьютере, в том числе переименованную учетную запись гостя.

Применение политики безопасности для объекта групповой политики рабочей компьютера, присоединенного к домену Windows Server 2008 R2

В этом примере мы запретим пользователю Test_ADUser изменять пароль для учетной записи на своем компьютере. Напомню, что для выполнения следующих действий вы должны входить в группу **«Администраторы домена»**. Выполните следующие действия:

1. Откройте **«Консоль управления ММС»**. Для этого нажмите на кнопку **«Пуск»**, в поле поиска введите *mmc*, а затем нажмите на кнопку **«Enter»**;
2. В меню **«Консоль»** выберите команду **«Добавить или удалить оснастку»** или воспользуйтесь комбинацией клавиш **Ctrl+M**;
3. В диалоге **«Добавление и удаление оснасток»** выберите оснастку **«Редактор локальной групповой политики»** и нажмите на кнопку **«Добавить»**;
4. В появившемся диалоге **«Выбор объекта групповой политики»** нажмите на кнопку **«Обзор»** для выбора компьютера и выберите нужный компьютер;
5. В диалоге **«Выбор объекта групповой политики»** убедитесь, что выбрали нужный компьютер и нажмите на кнопку **«Готово»**;
6. В диалоге **«Добавление или удаление оснасток»** нажмите на кнопку **«ОК»**;
7. В оснастке **«Редактор локальной групповой политики»** перейдите в узел **«Конфигурация компьютера»**, а затем откройте узел **Параметры безопасности\Локальный компьютер\Параметры безопасности**;
8. Откройте параметр **«Контроллер домена: Запретить изменение пароля учетных записей компьютера»** дважды щелкнув на нем или нажав на клавишу **Enter**;
9. В диалоге настроек параметра политики безопасности выберите опцию **«Включить»** и нажмите на кнопку **«ОК»**;
10. Перезагрузите компьютер.

После перезагрузки компьютера для того чтобы проверить, применилась ли политика безопасности, перейдите на компьютер, над которым проводились изменения и откройте консоль управления MMC. В ней добавьте оснастку **«Локальные пользователи и группы»** и попробуйте изменить пароль для своей доменной учетной записи.

Применение политики безопасности для объекта групповой политики с контроллера домена Windows Server 2008 R2

При помощи этого примера, изменим число новых уникальных паролей, которые должны быть назначены учетной записи пользователя до повторного использования старого пароля. Эта политика позволяет вам улучшать безопасность, гарантируя, что старые пароли не будут повторно использоваться в течении нескольких раз. Войдите на контроллер домена или используйте средства администрирования удаленного сервера. Выполните следующие действия:

1. Откройте консоль **«Управление групповой политикой»** - в диалоговом окне **«Выполнить»**, в поле **«Открыть»** введите *gpmc.msc* и нажмите на кнопку **«ОК»**;
2. В контейнере **«Объекты групповой политики»** щелкните правой кнопкой мыши и из контекстного меню выберите команду **«Создать»**;
3. В поле **«Имя»** введите название объекта GPO, например **«Объект политики, предназначенный для тестирования»** и нажмите на кнопку **«ОК»**;
4. Щелкните правой кнопкой мыши на созданном объекте и из контекстного меню выберите команду **«Изменить»**;
5. В окне **«Редактор управления групповыми политиками»** разверните узел **Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей**;
6. Откройте параметр **«Вести журнал паролей»** дважды щелкнув на нем или нажав на клавишу **Enter**;
7. В диалоге настройки параметра политики установите флажок на опции **«Определить следующий параметр политики»**, в тестовом поле введите 5 и нажмите на кнопку **«ОК»**;
8. Закройте оснастку **«Редактор управления групповыми политиками»**.

9. В консоли **«Управление групповой политикой»** нажмите правой кнопкой мыши на группе безопасности, для которой будут применяться изменения, и из контекстного меню выберите команду **«Связать существующий объект групповой политики…»**. В диалоге **«Выбор объекта групповой политики»** выберите созданный вами объект;

10. В фильтрах безопасности объекта политики выберите пользователя или группу, на которых будет распространяться указанные настройки.

11. Обновите параметры политики на клиентском компьютере при помощи команды **gpupdate**.

Об использовании оснастки **«Управление групповой политикой»** на контроллерах домена и о команде **gpupdate** будет подробно рассказываться в следующих разделах.

2.3.4. Политики учетных записей

Политика паролей

В организациях вы можете применять одинаковые политики паролей для всех пользователей, входящих в домен или только для отдельных групп при помощи оснастки **«Консоль управления групповыми политиками»**. В узле **«Политика паролей»** вы можете использовать до шести политик безопасности, при помощи которых можно указать наиболее важные параметры безопасности, применяемые для управления паролями учетных записей. Настоятельно рекомендую не игнорировать данные политики. Даже если вы уговорите своих пользователей использовать сложные пароли, не факт, что они действительно будут это делать. Если вы правильно настроите все шесть политик безопасности, расположенных в этом узле, безопасность паролей пользователей вашей организации значительно повысится. Применив все политики, пользователям действительно придется создавать безопасные пароли, в отличие от тех, которые они считают «сложными». Доступны следующие политики безопасности:

Вести журнал паролей. Насколько не был бы ваш пароль безопасным, злоумышленник рано или поздно сможет его подобрать. Поэтому необходимо периодически изменять пароли учетных записей. При помощи этой политики вы можете указать количество новых паролей, которые назначаются для учетных записей до повторного ис-

пользования старого пароля. После того как эта политика будет настроена, контроллер домена будет проверять кэш предыдущих хэш-кодов пользователей, чтобы в качестве нового пароля пользователи не могли использовать старый. Число паролей может варьироваться от 0 до 24. Т.е., если вы указали в качестве параметра число 24, то пользователь сможет использовать старый пароль с 25-ого раза.

Максимальные срок действия пароля. Эта политика указывает период времени, в течение которого пользователь может использовать свой пароль до последующего изменения. По окончанию установленного срока пользователь обязан изменить свой пароль, так как без изменения пароля войти в систему ему не удастся. Доступные значения могут быть установлены в промежутке от 0 до 999 дней. Если установлено значения равное 0, срок действия пароля неограничен. В связи с мерами безопасности желательно отказаться от такого выбора. Если значения максимального срока действия пароля варьируется от 1 до 999 дней, значение минимального срока должно быть меньше максимального. Лучше всего использовать значения от 30 до 45 дней.

Минимальная длина пароля. При помощи этой политики вы можете указать минимальное количество знаков, которое должно содержаться в пароле. Если активировать этот параметр, то при вводе нового пароля количество знаков будет сравниваться с тем, которое установлено в этой политике. Если количество знаков будет меньше указанного, то придется изменить пароль в соответствии с политикой безопасности. Можно указать значение политики от 1 до 14 знаков. Оптимальным значением для количества знаков для пароля пользователей является 8, а для серверов от 10 до 12.

Минимальные срок действия пароля. Многие пользователи не захотят утруждать себя запоминанием нового сложного пароля и могут попробовать сразу при вводе изменить такое количество новых паролей, чтобы использовать свой хорошо известный первоначальный пароль. Для предотвращения подобных действий была разработана текущая политика безопасности. Вы можете указать минимальное количество дней, в течение которого пользователь должен использовать свой новый пароль. Доступные значения этой политики устанавливаются в промежутке от 0 до 998 дней. Установив значение равное 0 дней, пользователь сможет изменить пароль сразу после создания нового. Необходимо обратить внимание на то, что минимальный срок действия нового пароля не должен превышать значение максимального срока действия.

Пароль должен отвечать требованиям сложности. Это одна из самых важных политик паролей, которая отвечает за то, должен ли пароль соответствовать требованиям сложности при создании или изменении пароля. В связи с этими требованиями, пароли должны:

содержать буквы верхнего и нижнего регистра одновременно;

содержать цифры от 0 до 9;

содержать символы, которые отличаются от букв и цифр (например, !, @, #, $, *);

Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

В том случае, если пользователь создал или изменил пароль, который соответствует требованиям, то пароль пропускается через математический алгоритм, преобразовывающий его в хэш-код (также называемый односторонней функцией), о котором шла речь в политике **«Вести журнал паролей».**

Хранить пароли, используя обратимое шифрование. Для того чтобы пароли невозможно было перехватить при помощи приложений, Active Directory хранит только хэш-код. Но если перед вами встанет необходимость поддержки приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности, вы можете использовать текущую политику. Обратимое шифрование по умолчанию отключено, так как, используя эту политику, уровень безопасности паролей и всего домена в частности значительно понижается. Использование этой функции аналогично хранению пароля в открытом виде.

Политика блокировки учетной записи

Даже после создания сложного пароля и правильной настройки политик безопасности, учетные записи ваших пользователей все еще могут быть подвергнуты атакам недоброжелателей. Например, если вы установили минимальный срок действия пароля в 20 дней, у хакера достаточно времени для подбора пароля к учетной записи. Узнать имя учетной записи не является проблемой для хакеров, так как, зачастую имена учетных записей пользователей совпадает с именем адреса почтового ящика. А если будет известно имя, то для подбора пароля понадобится какие-то две-три недели.

Групповые политики безопасности Windows могут противостоять таким действиям, используя набор политик узла **«Политика блокировки учетной записи»**. При помощи данного набора политик, у вас есть возможность ограничения количества некорректных попыток входа пользователя в систему. Разумеется, для ваших пользователей это может быть проблемой, так как не у всех получится ввести пароль за указанное количество попыток, но зато безопасность учетных записей перейдет на «новый уровень». Для этого узла доступны только три политики:

Время до сброса счетчиков блокировки. Active Directory и групповые политики позволяют автоматически разблокировать учетную запись, количество попыток входа в которую превышает установленное вами пороговое значение. При помощи этой политики устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Вы можете установить значение от одной минуты до 99999. Это значение должно быть меньше значения политики **«Продолжительность блокировки учетной записи»**.

Пороговое значение блокировки. Используя эту политику, вы можете указать количество некорректных попыток входа, после чего учетная запись будет заблокирована. Окончание периода блокировки учетной записи задается политикой **«Продолжительность блокировки учетной записи»** или администратор может разблокировать учетную запись вручную. Количество неудачных попыток входа может варьироваться от 0 до 999. Рекомендуется устанавливать допустимое количество от трех до семи попыток.

Продолжительность блокировки учетной записи. При помощи этого параметра вы можете указать время, в течение которого учетная запись будет заблокирована до ее автоматической разблокировки. Вы можете установить значение от 0 до 99999 минут. В том случае, если значение этой политики будет равно 0, учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную.

Политика Kerberos

В доменах Active Directory для проверки подлинности учетных записей пользователей и компьютеров домена используется протокол Kerberos. Сразу после аутентификации пользователя или компьютера, этот протокол проверяет подлинность указанных реквизитов, а затем выдает особый пакет данных, который называется **«Билет предостав-**

ления билета (TGT – Ticket Granting Ticket)». Перед подключением пользователя к серверу для запроса документа на контроллер домена пересылается запрос вместе с билетом TGT, который идентифицирует пользователя, прошедшего проверку подлинности Kerberos. После этого контроллер домена передает пользователю еще один пакет данных, называемый билетом доступа к службе. Пользователь предоставляет билет на доступ службе на сервере, который принимает его как подтверждение прохождения проверки подлинности.

Данный узел вы можете обнаружить только на контроллерах домена. Доступны следующие пять политик безопасности:

Максимальная погрешность синхронизации часов компьютера. Для предотвращения «атак повторной передачи пакетов» существует текущая политика безопасности, которая определяет максимальную разность времени, допускающую Kerberos между временем клиента и временем на контроллере домена для обеспечения проверки подлинности. В случае установки данной политики, на обоих часах должны быть установлены одинаковые дата и время. Подлинной считается та отметка времени, которая используется на обоих компьютерах, если разница между часами клиентского компьютера и контроллера домена меньше максимальной разницы времени, определенной этой политикой.

Максимальный срок жизни билета пользователя. При помощи текущей политики вы можете указать максимальный интервал времени, в течение которого может быть использован билет представления билета (TGT). По истечении срока действия билета TGT необходимо возобновить существующий билет или запросить новый.

Максимальный срок жизни билета службы. Используя эту политику безопасности, сервер будет выдавать сообщение об ошибке в том случае, если клиент, запрашивающий подключение к серверу, предъявляет просроченный билет сеанса. Вы можете определить максимальное количество минут, в течение которого полученный билет сеанса разрешается использовать для доступа к конкретной службе. Билеты сеансов применяются только для проверки подлинности на новых подключениях к серверам. После того как подключение пройдет проверку подлинности, срок действия билета теряет смысл.

Максимальный срок жизни для возобновления билета пользователя. С помощью данной политики вы можете установить количе-

ство дней, в течение которых может быть восстановлен билет предоставления билета.

Принудительные ограничения входа пользователей. Эта политика позволяет определить, должен ли центр распределения ключей Kerberos проверять каждый запрос билета сеанса на соответствие политике прав, действующей для учетных записей пользователей.

2.3.5. Политики аудита

Все попытки вторжения и неудачную аутентификацию ваших пользователей необходимо фиксировать для того чтобы знать, нужно ли предпринимать дополнительные меры по обеспечению безопасности. Проверка такой информации с целью определения активности на предприятии называется аудитом.

В процессе аудита используются три средства управления: политика аудита, параметры аудита в объектах, а также журнал **«Безопасность»**, куда заносятся события, связанные с безопасностью, такие как вход/выход из системы, использование привилегий и обращение к ресурсам. В этом разделе мы рассмотрим именно политики аудита и последующий анализ событий в журнале **«Безопасность»**.

Политика аудита

Политика аудита настраивает в системе определенного пользователя и группы аудит активности. Для того чтобы отконфигурировать политики аудита, в редакторе управления групповыми политиками вы должны открыть узел **Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Локальные политики/Политика аудита**. Необходимо помнить, что по умолчанию параметр политики аудита, для рабочих станций установлен на **«Не определено»**.

Так же, как и с остальными политиками безопасности, для настройки аудита вам нужно определить параметр политики. После двойного нажатия левой кнопкой мыши на любом из параметров, установите флажок на опции **«Определить следующие параметры политики»** и укажите параметры ведения аудита успеха, отказа или обоих типов событий.

После настройки политики аудита события будут заноситься в журнал безопасности. Просмотреть эти события можно в журнале безопасности. Рассмотрим подробно каждую политику аудита:

Аудит входа в систему. Текущая политика определяет, будет ли операционная система пользователя, для компьютера которого применяется данная политика аудита, выполнять аудит каждой попытки входа пользователя в систему или выхода из нее. Например, при удачном входе пользователя на компьютер генерируется событие входа учетной записи. События выхода из системы создаются каждый раз, когда завершается сеанс вошедшей в систему учетной записи пользователя. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Аудит доступа к объектам. Данная политика безопасности выполняет аудит попыток доступа пользователей к объектам, которые не имеют отношения к Active Directory. К таким объектам можно отнести файлы, папки, принтеры, разделы системного реестра, которые задаются собственными списками в системном списке управления доступом (SACL). Аудит создается только для объектов, для которых указаны списки управления доступом, при условии, что запрашиваемый тип доступа и учетная запись, выполняющая запрос, соответствуют параметрам в данных списках.

Аудит доступа к службе каталогов. При помощи этой политики безопасности вы можете определить, будет ли выполняться аудит событий, указанных в системном списке контроля доступа (SACL), который можно редактировать в диалоговом окне**«Дополнительные параметры безопасности»** свойств объекта Active Directory. Аудит создается только для объектов, для которых указан системный список управления доступом, при условии, что запрашиваемый тип доступа и учетная запись, выполняющая запрос, соответствуют параметрам в данном списке. Данная политика в какой-то степени похожа на политику **«Аудит доступа к объектам»**. Аудит успехов означает создание записи аудита при каждом успешном доступе пользователя к объекту Active Directory, для которого определена таблица SACL. Аудит отказов означает создание записи аудита при каждой неудачной попытке доступа пользователя к объекту Active Directory, для которого определена таблица SACL.

Аудит изменения политики. Эта политика аудита указывает, будет ли операционная система выполнять аудит каждой попытки изменения политики назначения прав пользователям, аудита, учетной записи или доверия. Аудит успехов означает создание записи аудита при каждом успешном изменении политик назначения прав пользова-

телей, политик аудита или политик доверительных отношений. Аудит отказов означает создание записи аудита при каждой неудачной попытке изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Аудит изменения привилегий. Используя эту политику безопасности, вы можете определить, будет ли выполняться аудит использования привилегий и прав пользователей. Аудит успехов означает создание записи аудита для каждого успешного применения права пользователя. Аудит отказов означает создание записи аудита для каждого неудачного применения права пользователя.

Аудит отслеживания процессов. Текущая политика аудита определяет, будет ли операционная система выполнять аудит событий, связанных с процессами, такими как создание и завершение процессов, а также активация программ и непрямой доступ к объектам. Аудит успехов означает создание записи аудита для каждого успешного события, связанного с отслеживаемым процессом. Аудит отказов означает создание записи аудита для каждого неудачного события, связанного с отслеживаемым процессом.

Аудит системных событий. Данная политика безопасности имеет особую ценность, так как именно при помощи этой политики вы можете узнать, перегружался ли у пользователя компьютер, превысил ли размер журнала безопасности пороговое значение предупреждений, была ли потеря отслеженных событий из-за сбоя системы аудита и даже вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени. Аудит успехов означает создание записи аудита для каждого успешного системного события. Аудит отказов означает создание записи аудита для каждого неудачного завершения системного события.

Аудит событий входа в систему. При помощи этой политики аудита вы можете указать, будет ли операционная система выполнять аудит каждый раз при проверке данным компьютером учетных данных. При использовании этой политики создается событие для локального и удаленного входа пользователя в систему. Члены домена и компьютеры, не входящие в домен, являются доверенными для своих локальных учетных записей. Когда пользователь пытается подключиться к общей папке на сервере, в журнал безопасности записывается событие удаленного входа, причем события выхода из системы не записываются. Аудит успехов означает создание записи аудита для каж-

дой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Аудит управления учетными записями. Эта последняя политика тоже считается очень важной, так как именно при помощи нее вы можете определить, необходимо ли выполнять аудит каждого события управления учетными записями на компьютере. В журнал безопасности будут записываться такие действия как создание, перемещение и отключение учетных записей, а также изменение паролей и групп. Аудит успехов означает создание записи аудита для каждого успешного события управления учетными записями. Аудит отказов означает создание записи аудита для каждого неудачного события управления учетными записями

Как видите, все политики аудита в какой-то степени очень похожи и если вы для каждого пользователя свой организации установите аудит всех политик, то рано или поздно вы просто запутаетесь в них. Поэтому необходимо вначале определить, что именно необходимо для аудита. Например, чтобы удостовериться в том, что к одной из ваших учетных записей постоянно пытаются получить несанкционированный доступ методом подбора пароля, вы можете указать аудит неудачных попыток входа. В следующем разделе мы рассмотрим простейший пример использования данных политик.

Пример использования политики аудита

Допустим, у нас есть домен testdomain.com, в котором есть пользователь с учетной записью DImaN.Vista. в данном примере мы применим для этого пользователя политику **«Аудит событий входа в систему»** и увидим, какие события записываются в журнал безопасности при попытке несанкционированного доступа в систему. Для воспроизведения подобной ситуации выполните следующие действия:

1. На контроллере домена создайте пользовательскую учетную запись и поместите ее в группу безопасности «Vista», которая расположена в подразделении **«Группы»**;
2. Откройте консоль **«Управление групповой политикой»**, где выберите контейнер **«Объекты групповой политики»** и нажмите на этом контейнере правой кнопкой мыши для отображения контекстного меню;
3. В контекстном меню выберите команду **«Создать»** и в отобразившемся диалоговом окне **«Новый объект групповой политики»** введите **«Политика аудита»**, после чего нажмите кнопку **«ОК»**;

4. Выберите данный объект групповой политики и из контекстного меню выберите команду **«Изменить»**;

5. В появившемся окне **«Редактор управления групповыми политиками»** разверните узел **Конфигурация компьютера/Политика/Конфигурация Windows/Параметры безопасности/Локальные политики/Политика аудита** и откройте параметр политики **«Аудит событий входа в систему»**;

6. Установите флажки возле опций **«Определить следующие параметры политики»** и **«отказ»** и нажмите на **«ОК»**;

7. Закройте редактор управления групповыми политиками;

8. Свяжите объект **«Политики аудита»** с подразделением **«Группы»**. Для этого щелкните правой кнопкой мыши на подразделение **«Группы»** и из контекстного меню выберите команду **«Связать существующий объект групповой политики»**;

9. В диалоговом окне **«Выбор объекта групповой политики»** выберите объект **«Политика аудита»** и нажмите на кнопку **«ОК»**;

10. Разверните подразделение **«Группы»** и в области **«Фильтры безопасности»** удалите фильтр **«Прошедшие проверку»**. После этого нажмите на кнопку **«Добавить»** и выберите группу **«Vista»**, которую мы создавали ранее;

11. Перейдите на клиентскую машину и обновите групповые политики при помощи команды gpupdate;

12. Заблокируйте компьютер и попробуйте войти в систему, используя заведомо неправильный пароль;

13. На контроллере домена откройте оснастку **«Просмотр событий»** и перейдите в журнал **«Безопасность»**;

14. Проверьте, как сгенерировалось сообщение аудита отказа.

2.3.6. Назначение прав пользователей

Стоит учесть, что пользователи не владеют достаточной базой знаний по обеспечению безопасности и даже у обычного пользователя может быть достаточно привилегий для нанесения ущерба своей системе и даже компьютерам в вашей интрасети. Избежать подобных проблем помогают локальные политики безопасности назначения прав пользователя, о чем, собственно, и пойдет речь в данном разделе. При помощи политик назначения прав пользователя вы можете сами определить, для каких пользователей или групп пользователей будут предоставлены различные права и привилегии. Оперируя данными политиками, вы можете не волноваться за то, что пользователи будут выполнять действия, которые им делать не положено. Далее вы смо-

жете ознакомиться с политиками безопасности, которые отвечают за назначение различных прав для пользователей или групп вашей организации.

Архивация файлов и каталогов. При помощи данной политики вы можете указать пользователей или группы, предназначенные для выполнения операций резервного копирования файлов, каталогов, разделов реестра и других объектов, которые подлежат архивации. Данная политика предоставляет доступ для следующих разрешений:

- Обзор папок/Выполнение файлов
- Содержимое папки/Чтение данных
- Чтение атрибутов
- Чтение расширенных атрибутов
- Чтение разрешений

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**, а на контроллерах домена – **«Операторы архивации»** и **«Операторы сервера»**.

Блокировка страниц в памяти. Используя эту политику безопасности, вы можете указать конкретных пользователей или группы, которым разрешается использовать процессы для сохранения данных в физической памяти для предотвращения сброса данных в виртуальную память на диске.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

Восстановление файлов и каталогов. Эта политика позволяет вам указывать пользователей и группы, которые могут выполнять восстановление файлов и каталогов, в обход блокировке файлов, каталогов, разделов реестра и прочих объектов, расположенных в архивных версиях файлов.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**, а на контроллерах домена – **«Операторы архивации»** и **«Операторы сервера»**.

Вход в качестве пакетного задания. При создании задания, используя планировщик заданий, операционная система регистрирует пользователя в системе как пользователя с пакетным входом. Данная

политика разрешает группе или определенному пользователю входить в систему при помощи такого метода.

По умолчанию, как на рабочих станциях, так и на контроллерах домена, данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**.

Вход в качестве службы. Некоторые системные службы осуществляют вход в операционную систему под разными учетными записями. Например, служба **«Windows Audio»** запускается под учетной записью **«Локальная служба»**, служба **«Телефония»** использует учетную запись **«Сетевая служба»**. Данная политика безопасности определяет, какие учетные записи служб могут зарегистрировать процесс в качестве службы.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

Выполнение задач по обслуживанию томов. Используя эту политику, вы можете указать пользователей или группы, участники которых могут выполнять операции, предназначенные для обслуживания томов. У пользователей, обладающих такими привилегиями, есть права на чтение и изменение запрошенных данных после открытия дополнительных файлов, они также могут просматривать диски и добавлять файлы в память, занятую другими данными.

По умолчанию, такими правами обладают только администраторы рабочих станций и контроллеров домена.

Добавление рабочих станций к домену. Эта политика отвечает за разрешение пользователям или группам добавлять компьютеры в домен Active Directory. Пользователь, обладающий данными привилегиями, может добавить в домен до десяти компьютеров.

По умолчанию, все пользователи, прошедшие проверку подлинности, на контроллерах домена могут добавлять до десяти компьютеров.

Доступ к диспетчеру учетных данных от имени доверенного вызывающего. Диспетчер учетных данных – это компонент, который предназначен для хранения учетных данных, таких как имена пользователей и пароли, используемых для входа на веб-сайты или другие компьютеры в сети. Эта политика используется диспетчером учетных

данных в ходе архивации и восстановления, и ее не желательно предоставлять пользователям.

По умолчанию, как на рабочих станциях, так и на серверах, ни у одной группы нет на это разрешений.

Доступ к компьютеру из сети. Данная политика безопасности отвечает за разрешение подключения к компьютеру по сети указанным пользователям или группам.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Операторы архивации»**, **«Пользователи»** и **«Все»**. На контроллерах домена – **«Администраторы»**, **«Проверенные пользователи»**,**«Контроллеры домена предприятия»** и **«Все»**.

Завершение работы системы. Используя этот параметр политики, вы можете составить список пользователей, которые имеют право на использование команды **«Завершение работы»** после удачного входа в систему.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»**, **«Операторы архивации»** и **«Пользователи»** (только на рабочих станциях), а на контроллерах домена – **«Администраторы»**, **«Операторы архивации»**, **«Операторы сервера»** и **«Операторы печати»**.

Загрузка и выгрузка драйверов устройств. При помощи текущей политики вы можете указать пользователей, которым будут предоставлены права на динамическую загрузку и выгрузку драйверов устройств в режиме ядра, причем эта политика не распространяется на PnP-устройства.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»**, а на контроллерах домена – **«Администраторы»** и **«Операторы печати»**.

Замена маркера уровня процесса. Используя данную политику безопасности, вы можете ограничить пользователей или группу от использования API-функции CreateProcessAsUser для того, чтобы одна служба могла запускать другую функцию, процесс или службу. Стоит обратить внимание на то, что такое приложение как **«Планировщик заданий»** для своей работы использует данные привилегии.

По умолчанию, как на рабочих станциях, так и на контроллерах домена, данные привилегии предоставляются учетным записям **«Сетевая служба»** и **«Локальная служба»**.

Запретить вход в систему через службу удаленных рабочих столов. При помощи данной политики безопасности вы можете ограничить пользователей или группы от входа в систему в качестве клиента удаленных рабочих столов.

По умолчанию, как на рабочих станциях, так и на серверах, всем разрешено входить в систему как клиенту удаленных рабочих столов.

Запретить локальный вход. Данная политика запрещает отдельным пользователям или группам выполнять вход в систему.

По умолчанию всем пользователям разрешен вход в систему.

Изменение метки объектов. Благодаря данной политике назначения прав, вы можете предоставить возможность указанным пользователям или группам изменять метки целостности объектов других пользователей, таких как файлы, разделы реестра или процессы.

По умолчанию никому не разрешено изменять метки объектов.

Изменение параметров среды изготовителя. Используя эту политику безопасности, вы можете указать пользователей или группы, которым будет доступна возможность чтения переменных аппаратной среды. Переменные аппаратной среды - это параметры, сохраняемые в энергонезависимой памяти компьютеров, архитектура которых отлична от x86.

На рабочих станциях и контроллерах домена, по умолчанию данные привилегии предоставляются группам **«Администраторы»**.

Изменение системного времени. Эта политика отвечает за изменение системного времени. Предоставив данное право пользователям или группам, вы тем самым кроме разрешения изменения даты и времени внутренних часов позволите им изменять соответствующее время отслеживаемых событий в оснастке **«Просмотр событий»**.

На рабочих станциях и серверах данные привилегии предоставляются группам **«Администраторы»** и **«Локальная служба»**, а на контроллерах домена – **«Администраторы»**, **«Операторы сервера»** и **«Локальная служба»**.

Изменение часового пояса. При помощи текущей политики безопасности, вы можете указать пользователей или группы, которым разрешено изменять часовой пояс своего компьютера для отображения местного времени, которое представляет собой сумму системного времени компьютера и смещения часового пояса.

На рабочих станциях и контроллерах домена по умолчанию данные привилегии предоставляются группам **«Администраторы»** и **«Пользователи»**.

Применение политик назначение прав пользователей

В этом примере будет показано, как можно назначить права для одной из групп вашей организации на контроллере домена. Выполните следующие действия:

1. Откройте оснастку **«Управление групповой политикой»** и выберите контейнер, к которому будут привязаны политики назначения прав пользователей, например, **«Группы»**;
2. Нажмите правой кнопкой мыши на контейнере и из контекстного меню выберите команду **«Создать объект групповой политики в этом домене и связать его…»**. В диалоговом окне **«Новый объект групповой политики»** введите **«Права для группы отладчиков»** и нажмите на кнопку **«ОК»**;
3. Выделите созданный объект групповой политики, нажмите на нем правой кнопкой мыши и из контекстного меню выберите команду **«Изменить»;**
4. В окне **«Редактор управления групповыми политиками»**, в дереве консоли разверните узел **«Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя»**;
5. Откройте свойства политики **«Отладка программ»**. При помощи этой политики, пользователи смогут выполнять отладку системных компонентов, что обеспечивает полный доступ к компонентам операционной системы. На вкладке **«Параметр политики безопасности»** установите флажок на опции **«Определить следующие параметры политики»** и нажмите на кнопку **«Добавить пользователя или группу»**;

6. В диалоговом окне **«Добавление пользователя или группы»** нажмите на кнопку **«Обзор»**. В поле **«Введите имя выбираемых объектов»** укажите название группы (в данном случае – **«Отладчики»**) и нажмите на кнопку **«Проверить имена»**. Если вы не помните название группы, нажмите на кнопку «Дополнительно» и выполните поиск при помощи поисковых запросов;

7. Нажмите два раза на кнопку **«ОК»**;

8. Закройте редактор управления групповыми политиками. В оснастке **«Управление групповыми политиками»** на вкладке **«Область»** в фильтрах безопасности удалите группу **«Прошедшие проверку»**. Затем нажмите на кнопку **«Добавить»** и выберите группу **«Отладчики»**;

9. На компьютерах пользователей, которые входят в группу **«Отладчики»** инициируйте обновление групповых политик при помощи команды Gpupdate.

2.3.7. Политики журнала событий

Для того чтобы перейти к настройке политик журналов событий, в редакторе управления групповыми политиками откройте узел **Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Локальные политики/Журнал событий**.

Рассмотрим подробно каждую политику данного узла:

Запретить доступ для локальной группы гостей к журналу безопасности. Данная политика безопасности может быть применена только к операционным системам, которые предшествуют Windows Vista. Применяется данная политика с целью ограничения локальной группы гостей, использующих анонимный вход в систему для журнала безопасности в операционных системах Windows XP и Windows 2000. По умолчанию, для клиентов, использующих операционную систему Windows 2000, данная политика отключена, а для пользователей Windows XP – включена.

Запретить доступ для локальной группы гостей к журналу приложений. Действия этой политики безопасности аналогичны политике **«Запретить доступ для локальной группы гостей к журналу безопасности»**. Эта политика отличается от предыдущей только тем, что используя параметры текущей политики, вы можете ограничить

гостевых пользователей в доступе к журналу **«Приложения»**. По умолчанию, для клиентов, использующих операционную систему Windows 2000, данная политика отключена, а для пользователей Windows XP – включена.

Запретить доступ для локальной группы гостей к системному журналу. Текущая политика безопасности также как и две предыдущих политики, позволяет пользователям операционных систем Windows XP и Windows 2000 запрещать локальным гостям с анонимным входом в систему иметь доступ к журналу **«Система»**. По умолчанию, для клиентов, использующих операционную систему Windows 2000, данная политика отключена, а для пользователей Windows XP – включена.

Максимальный размер журнала безопасности. Если вам нужно указать максимальный размер определенного журнала для целой группы пользователей, то вы можете упростить себе эту задачу и воспользоваться текущей политикой безопасности. Эта политика безопасности позволяет указывать максимальный размер журнала «Безопасность». Максимальный размер журнала может достигать 4 Гб, но обычно указывают максимальный размер не более 500 Мб. Ограничение размера журнала безопасности может привести к затиранию важных событий, так как по достижению порогового объема, у вас будут удаляться самые старые события, и вместо них будут записываться новые. Размеры файлов журнала должны быть кратны 64 КБ. Если введено значение, не кратное 64 КБ, средство просмотра событий установит размер файла журнала, кратный 64 КБ. Обычно, есть смысл увеличивать размер журнала событий только в том случае, если есть необходимость в тщательной обработке событий безопасности и сохранении журнала на протяжении длительного периода времени. По умолчанию в операционной системе Windows 7 и Windows Vista размер журнала безопасности составляет 20 Мб, в Windows Server 2008 и Windows Server 2008 R2 – 128 Мб, для операционных систем Windows Server 2003 – 16 Мб, а Windows XP – 8 Мб.

Максимальный размер журнала приложений. Настройки этой политики безопасности идентичны настройкам предыдущей политики за исключением того, что здесь вы можете указать максимальный размер журнала «Приложения» для компьютеров и пользователей на которых будет распространена область действия объекта групповой политики.

Максимальный размер системного журнала. От предыдущих двух политик безопасности данная политика отличается лишь тем, что она отвечает за максимальный размер журнала **«Система»**.

Метод сохранения событий в журнале безопасности. Данная политика безопасности напрямую связана с политиками **«Максимальный размер журнала безопасности»** и **«Сохранять события в журнале безопасности»** в связи с тем, что эта политика отвечает за перезапись журнала безопасности по превышению установленного лимита на размер. Для вас доступно одно из трех значений. При выборе значения **«Затирать события по необходимости»**, по истечению свободного места в журнале, все старые события будут удаляться, и перезаписываться новыми. Обычно это значение используется в том случае, если у вас нет необходимости в архивировании событий указанного журнала. Значение **«Затирать события по дням»** целесообразно использовать в том случае, если у вас выполняется архивирование журнала по заданному промежутку времени, которое указывается при помощи политики **«Сохранять события в журнале безопасности»**. В этом случае будут удаляться все события в данном журнале по истечении указанного срока. Также в этом случае стоит обратить внимание на то, чтобы максимальный размер журнала позволял вам сохранять все события за указанный промежуток времени. Значение **«Не затирать события (чистка журнала вручную)»**обычно используется в том случае, когда есть необходимость в сохранении всех событий непосредственно в журнале. Но стоит учесть, что после того как журнал достигнет максимального размера, все новые события будут просто отклоняться.

Метод сохранения событий в журнале приложений. Параметры этой политики безопасности идентичны настройкам предыдущей политики за исключением того, что здесь вы можете указать настройки сохранения событий для журнала **«Приложения»** компьютеров и пользователей, на которых будет распространена область действия объекта групповой политики.

Метод сохранения событий в системном журнале. Эта политика безопасности предназначена для настройки сохранения событий в журнале **«Система»**.

Сохранять события в журнале безопасности. Текущая политика безопасности определяет, как долго могут сохраняться события в журнале **«Безопасность»** в том случае, если для политики **«Метод сохранения событий в журнале безопасности»**указано значение **«За-**

тирать события по дням». Помимо этого вам нужно убедиться в том, что размер вашего журнала позволяет сохранять события за указанный промежуток времени, так как после достижения журналом максимального размера, все новые события будут просто отклоняться.

Сохранять события в журнале приложений. Эта политика безопасности предназначена для определения количества дней, на протяжении которых в журнале **«Приложения»** будут сохраняться события.

Сохранять события в системном журнале. Параметры этой политики безопасности идентичны настройкам предыдущих двух политик за исключением того, что здесь вы можете указать период времени хранения событий для журнала **«Система»** компьютеров и пользователей, на которых будет распространена область действия объекта групповой политики.

Примеры использования политик журналов событий

Разберемся с настройками политик безопасности журналов событий на живом примере. В этом примере мы определим настройки журналов событий **«Приложения»**, **«Безопасность»** и **«Система»** для группы **«Бухгалтерия»** организации. Предположим, что в вашем отделе бухгалтерии все компьютеры оснащены операционными системами Windows Vista и Windows 7, в связи с чем, параметры политики **«Запретить доступ для локальной группы гостей к журналу ...»** не будут задействованы. Выполните следующие действия:

1. На контроллере домена создайте группу безопасности **«Бухгалтерия»** и поместите ее в подразделение **«Группы»**;
2. Откройте консоль **«Управление групповой политикой»**, где выберите контейнер **«Объекты групповой политики»** и нажмите на этом контейнере правой кнопкой мыши для отображения контекстного меню;
3. В контекстном меню выберите команду **«Создать»** и в отобразившемся диалоговом окне **«Новый объект групповой политики»** введите **«Политики журналов событий для отдела бухгалтерии»**, после чего нажмите кнопку **«ОК»**;
4. Выберите данный объект групповой политики и из контекстного меню выберите команду **«Изменить»**;
5. В появившемся окне **«Редактор управления групповыми политиками»** разверните узел **Конфигурация компьюте-**

ра/Политика/Конфигурация Windows/Параметры безопасности/Журнал событий и выберите политику **«Максимальный размер журнала безопасности»**;

6. В диалоговом окне **«Свойства: Максимальный размер журнала безопасности»** установите флажок **«Определить следующий параметр политики»** и в соответствующем текстовом поле установите значение в 30 МБ, что равняется 30720 КБ;

7. Предположим, что в отделе безопасности установлены надежные пароли, назначены все необходимые права для пользователей этой группы и у вас нет необходимости в аудите журналов безопасности этого отдела. Откройте свойства политики **«Метод сохранения событий в журнале безопасности»**. В диалоговом окне свойств политики установите флажок **«Определить следующий параметр политики»** и выберите значение **«Затирать старые события по необходимости»**. Теперь, по достижении 30 Мб самые старые события в журналах безопасности отдела бухгалтерии будут перезаписываться новыми;

8. Для журналов приложений группы бухгалтерии регистрируется не очень много событий, поэтому в настройках политики **«Максимальный размер журнала приложений»** укажем значение 25600 КБ, что равняется 25 МБ;

9. Вы не хотите, чтобы журнал **«Приложения»** для отдела бухгалтерии вашей организации перезаписывался, но не ведете его архивацию. Допустим, вы периодически его просматриваете и очищаете вручную. Для этого в политике **«Метод сохранения событий в журнале приложений»** установите значение **«Не затирать события (чистка журнала вручную)»**. Но вам необходимо учесть, что если вы не будете самостоятельно чистить данный журнал, то, в конечном счете, новые события не будут фиксироваться в журналах приложений отдела бухгалтерии;

10. Последний журнал, который вам предстоит настроить – это журнал **«Система»**. В политике **«Максимальный размер системного журнала»** установите размер 20 МБ, что является 20480 КБ;

11. По требованиям безопасности вашей организации вам необходимо создавать архивные копии системных журналов для всех групп

безопасности. Поэтому в политике **«Метод сохранения событий в системном журнале»** выберите значение **«Затирать старые события по дням»**. По нажатию на кнопку **«ОК»** перед вами будет отображен диалог **«Предлагаемые изменения значений»**, в котором указывается, что для политики **«Сохранять события в системном журнале»** будет установлено значение 7 дней. Это значение как раз соответствует требованиям по архивации системного значения и по нажатию закрытия данного диалога не будет необходимости в редактировании этой политики безопасности;

12. Закройте оснастку **«Редактор управления групповыми политиками».** После этого вам нужно привязать отредактированный объект групповой политики к группе безопасности **«Бухгалтерия»**. Для этого в оснастке **«Управление групповой политикой»** выберите контейнер **«Группы»**, нажмите на нем правой кнопкой мыши и из контекстного меню выберите команду **«Связать существующий объект групповой политики…»**. В диалоговом окне **«Выбор объекта групповой политики»** выберите объект **«Политики журналов событий для отдела бухгалтерии»** и нажмите на кнопку **«ОК»**;

13. Разверните подразделение **«Группы»**, выберите объект **«Политики журналов событий для отдела бухгалтерии»** и на вкладке **«Область»**, и в области **«Фильтры безопасности»** удалите фильтр **«Прошедшие проверку»**. После этого нажмите на кнопку **«Добавить»** и выберите группу **«Бухгалтерия»**, которая заранее была создана;

14. Перейдите на клиентские машины и обновите групповые политики, используя команду **Gpupdate**;

2.3.8. Политики системы

В этом разделе вы узнаете еще о четырех узлах локальных политик безопасности, а именно об управлении группами с ограниченным доступом, системных службах пользователей, которые попадают в область действия групповых политик, об ограничениях разделов системного реестра, а также о разрешениях файловой системы ваших рабочих станций. Эти политики безопасности позволят вам задать свойства для групп со специфическими требованиями, принудительно запускать или отключать службы согласно корпоративным требованиям, ограничить доступ к конкретным разделам системного реестра и управ-

лять разрешениями доступа и параметрами аудита для файловой системы. Правильное использование этих политик безопасности позволит вам закрыть множество уязвимостей, от злоумышленников, которым все-таки удалось проникнуть в системы ваших пользователей, а также от самих пользователей, которые в связи с некомпетентностью могут нанести не менее значительный ущерб своему компьютеру и рабочим станциям организации в частности. Все четыре указанных ниже локальных политик безопасности вы не сможете найти в оснастке **«Редактор локальной групповой политики»** клиентских операционных систем.

Группы с ограниченным доступом

При помощи локальных политик безопасности и политик **«Группы с ограниченным доступом»** в частности, вы можете указать два свойства, определяющие членов данной группы, а также членства в группах для конкретной группы безопасности. Данная политика безопасности имеет особенную ценность для организаций, в которых присуща сложная иерархия групп безопасности. Как известно, группы – это важный класс объектов, поскольку они служат для единого управления коллекциями пользователей, компьютеров и других групп. Несмотря на то, что данные политики безопасности очень похожи на возможности функционала оснастки **«Active Directory: Локальные пользователи и компьютеры»**, рекомендуется не игнорировать использование данных политик. В связи с тем, что на первый взгляд свойства **«Члены группы»** и **«Член групп»** очень похожи, между ними имеются существенные отличия.

Параметр **«Член групп»** указывает принадлежность данной группы к еще одной группе. Применение этого параметра гарантирует членство определяемой вами группы в указанной локальной группе. В том случае, если вы настроили локальные политики безопасности в нескольких объектах групповых политик, то для выбранных групп будет применяться каждый параметр членства группы. Например, если вы определили для группы **«Отдел разработки»**, что пользователи данной группы являются членами группы**«Разработчики»**, а второй объект, который привязан к дочернему подразделению, указывает что группа **«Отдел тестирования»** также является членом группы **«Разработчики»**, то, в конечном счете, обе группы будут принадлежать к группе**«Разработчики»**.

При помощи параметра **«Члены группы»**, вы можете указать членство в определяемой группе. Данный параметр является авторитарным, и он определяет окончательный список членов. Если политика групп с ограниченным доступом определена в нескольких объектах групповых политик, то объект GPO с высшим приоритетом будет иметь преимущества над остальными объектами групповых политик.

Например, попробуем настроить группу **«Отладчики»** как ограниченную группу, в которую входит группа **«Поддержка»**:

1. Откройте консоль **«Управление групповой политикой»**, где выберите контейнер **«Объекты групповой политики»** и нажмите на этом контейнере правой кнопкой мыши для отображения контекстного меню;
2. В контекстном меню выберите команду **«Создать»** и в отобразившемся диалоговом окне **«Новый объект групповой политики»** введите **«Группы с ограниченным доступом»**, после чего нажмите кнопку **«ОК»**;
3. Выберите данный объект групповой политики и из контекстного меню выберите команду **«Изменить»**;
4. В окне оснастки **«Редактор управления групповыми политиками»** разверните узел **Конфигурация компьютера/Политика/Конфигурация Windows/Параметры безопасности\Группы с ограниченным доступом** и вызовите диалоговое окно добавления группы одним из следующих методов:
5. В дереве консоли выберите узел **«Группы с ограниченным доступом»**, нажмите на нем правой кнопкой мыши и из контекстного меню выберите команду **«Добавить группу»**;
6. Нажмите правой кнопкой на панели сведений и из контекстного меню выберите команду **«Добавить группу»**;
7. Если у вас отображается панель действий, то перейдите в ней по ссылке **«Дополнительные действия»** и выберите команду **«Добавить группу»**.
8. В диалоговом окне **«Добавление группы»** в текстовом поле **«Группа»** введите название необходимой группы или найдите ее, вызвав диалоговое окно **«Выбор: Группы»**, нажав на кнопку **«Обзор»**, после чего нажмите на кнопку **«ОК»**;
9. В диалоговом окне **«TESTDOMAIN\Отладчики Свойства»** необходимо указать пользователей или группы, которые будут являться членами группы «Отладчики». Для этого возле области **«Члены этой группы»** нажмите на кнопку **«Добавить»**. Откроется такое же ок-

но, предназначенное для выбора группы, как и на предыдущем шаге. Выберем группу **«Поддержка»**, которая была создана заранее. В нашем случае, группа отладчиков не должна входить в какие-либо группы, поэтому далее нажмите на кнопку **«ОК»**.

10. Закройте оснастку **«Редактор управления групповыми политиками»**, привяжите измененный объект групповой политики к нужному вам контейнеру и установите область действия.

Системные службы

Узел **«Службы»** локальных политик безопасности отвечает за централизованное управление службами ваших клиентских машин. Для повышения производительности компьютеров вашей организации вы можете определить службы, которые будут запущены автоматически, которые нужно запускать вручную, а также службы, которые принудительно будут остановлены. Для того чтобы определить параметры служб, вам нужно выполнить следующие действия:

1. Откройте консоль **«Управление групповой политикой»**, где выберите контейнер **«Объекты групповой политики»** и нажмите на этом контейнере правой кнопкой мыши для отображения контекстного меню;
2. В контекстном меню выберите команду **«Создать»** и в отобразившемся диалоговом окне **«Новый объект групповой политики»** введите **«Службы для компьютеров организации»**, после чего нажмите кнопку **«ОК»**;
3. Выберите данный объект групповой политики и из контекстного меню выберите команду **«Изменить»**;
4. В окне оснастки **«Редактор управления групповыми политиками»** разверните узел **Конфигурация компьютера/Политика/Конфигурация Windows/Параметры безопасности\Системные службы**. Область сведений системных служб вы можете увидеть ниже:
5. Как видно из предыдущей иллюстрации, по умолчанию для всех системных служб установлено состояние **«Не определено»**. Для того чтобы настроить определенные системные службы, выберите любую службу, например, **«Служба ввода планшетного ПК»** и откройте ее свойства. Свойства данной службы отображены на следующей иллюстрации:
6. Установите флажок **«Определить следующий параметр политики»**, а затем установите переключатель на требуемое состояние.

Нажав на кнопку **«Изменить параметры»** вы можете указать параметры безопасности для групп и пользователей.

7. По окончанию настройки режима запуска службы нажмите на кнопку **«ОК»**.

8. Закройте оснастку **«Редактор управления групповыми политиками»**, привяжите измененный объект групповой политики к нужному вам контейнеру и установите область действия.

Реестр

Используя политики из узла **«Реестр»** вы можете определить права доступа и аудита для различных разделов системного реестра компьютеров, которые указаны в области действия объектов групповых политик. Для того чтобы запретить вашим пользователям изменять настройки автозапуска совместно с настройками режима запуска служб, выполните следующие действия:

Откройте консоль **«Управление групповой политикой»**, где выберите контейнер **«Объекты групповой политики»**, затем выберите объект групповой политики **«Службы для компьютеров организации»**, нажмите на нем правой кнопкой мыши и из контекстного меню выберите команду **«Изменить»**;

В появившемся окне оснастки **«Редактор управления групповыми политиками»** разверните узел **Конфигурация компьютера/Политика/Конфигурация Windows/Параметры безопасности\Реестр** и вызовите диалоговое окно **«Выбор раздела реестра»** из контекстного меню узла, области сведений, области действий или из меню **«Действие»**;

В диалоговом окне **«Выбор раздела реестра»**, введите в текстовом поле **«Выбранный реестр»** путь к требуемому разделу (в нашем случае - MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) или выберите необходимый раздел в области**«Реестр»**. Данное диалоговое окно вы можете увидеть ниже:

Нажмите на кнопку **«ОК»** для открытия диалогового окна управления безопасностью данного раздела. Выберите группу **«Пользователи»** и в области разрешений установите флажок для полного доступа на опцию **«Запретить»**. Вы можете добавить любую группу или пользователей по нажатию на кнопку **«Добавить»** или настроить дополнительные параметры безопасности. Нажмите на кнопку **«ОК»**;

В том случае, если вы задали элемент запрета разрешений, то перед вами отобразится предупреждение. Прочитайте его и нажмите на кнопку **«Да»** для продолжения выполнения операции.

В диалоговом окне **«Добавление объекта»** вы можете указать разрешения для всех дочерних разделов. Выберите необходимые разрешения и нажмите на кнопку **«ОК»**;

В области сведений будут отображаться все разделы реестра, для которых вы указали разрешения. По окончании добавления разделов реестра закройте оснастку **«Редактор управления групповых политик»**;

Файловая система

При помощи этого узла вы можете настроить разрешения доступа пользователям или группам к объектам, расположенных на данном компьютере. Принцип добавления объекта файловой системы полностью идентичен добавлению разрешений на разделы реестра за исключением того, что на третьем шаге вместо диалогового окна выбора раздела реестра вам нужно будет указать файл или папку в диалоговом окне **«Добавление файла или папки»**.

2.4. Шифрование в Windows. Технология BitLocker

Как вы уже знаете, когда операционная система находится в активном состоянии, ее можно защитить при помощи локальных политик безопасности, антивирусного программного обеспечения и брандмауэров с межсетевыми экранами, а вот защитить том операционной системы на жестком диске вы можете средствами шифрования.

Шифрование диска BitLocker – это средство безопасности в современных операционных системах Windows, которое позволяет защитить операционную систему и данные, которые хранятся на ваших компьютерах. В идеальном сочетании, BitLocker настраивается на использование доверенного платформенного модуля (TPM), что обеспечивает целостность компонентов начальной загрузки и блокировки томов, которые защищаются даже в том случае, если операционная система еще не запущена.

Для того чтобы воспользоваться всеми преимуществами шифрования BitLocker и проверки подлинности системы, компьютер должен соответствовать таким требованиям, как наличие установленного модуля TPM версии 1.2, который при включении шифрования позволяет

сохранять определенный ключ на съемном носителе для запуска системы. Помимо модуля TPM, в базовой системе ввода-вывода (BIOS) должна быть установлена спецификация группы Trusted Computing Group (TCG), которая перед загрузкой операционной системы создает цепочку доверий для действий и включает поддержку статического корневого объекта изменения уровня доверия. К сожалению, не все материнские платы оснащены таким модулем как TPM, но даже без этого модуля операционная система позволяет вам воспользоваться данной технологией шифрования при наличии запоминающих устройств USB с поддержкой команд UFI, а также в том случае, если ваш жесткий диск разбит на два и более тома. Например, на одном томе у вас будет находиться непосредственно операционная система для которой и будет включено шифрование, а второй, системный том, емкостью не менее 1,5Гб, содержит файлы, которые нужны для загрузки операционной системы после того как BIOS загрузит платформу. Все ваши томы должны быть отформатированы в файловой системе NTFS.

Архитектура шифрования BitLocker обеспечивает управляемые и функциональные механизмы, как в режиме ядра, так и в пользовательском режиме. На высоком уровне, к основным компонентам BitLocker можно отнести:

- Драйвер Trusted Platform Module (%SystemRoot%\System32\Drivers\Tpm.sys) – драйвер, который обращается к чипу TPM в режиме ядра;
- Основные службы TPM, которые включают пользовательские службы, предоставляющие доступ к TPM в пользовательском режиме (%SystemRoot%\System32\tbssvc.dll), поставщика WMI, а также оснастку MMC (%SystemRoot%\System32\Tpm.msc);
- Связанный код BitLocker в диспетчере загрузки (BootMgr), который аутентифицирует доступ к жесткому диску, а также позволяет восстанавливать и разблокировать загрузчик;
- Драйвер фильтра BitLocker (%SystemRoot%\System32\Drivers\Fvevol.sys), который позволяет шифровать и расшифровывать тома на лету в режиме ядра;
- Поставщик WMI BitLocker и управление сценариями, которые позволяют настраивать и управлять сценариями интерфейса BitLocker.

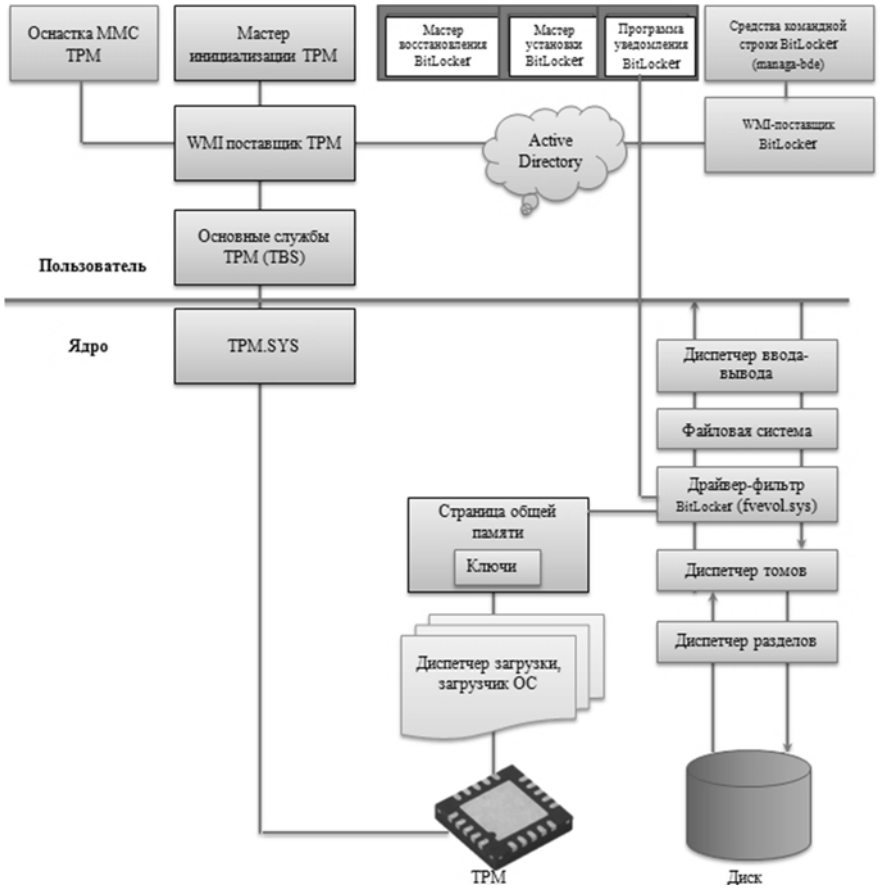
На следующей иллюстрации изображены различные компоненты и службы, которые обеспечивают корректную работу технологии шифрования BitLocker:

Ключи шифрования

BitLocker зашифровывает содержимое тома, используя ключ шифрования всего тома (FVEK – Full Volume Encryption Key), назначенного ему во время его первоначальной настройки для использования компонента BitLocker, с использованием алгоритмов 128- или 256-разрядного ключа AES AES128-CBC и AES256-CBC с расширениями Microsoft, которые называются диффузорами. Ключ FVEK шифруется с помощью главного ключа тома (VMK – Volume Master Key) и хранится на томе в области, специально отведенной для метаданных. Защита главного ключа тома является косвенным способом защиты данных тома: дополнение главного ключа тома позволяет системе пересоздать ключ после того как ключи были утеряны или скомпрометированы.

Когда вы настраиваете шифрование BitLocker, для защиты компьютера при помощи VMK, в зависимости от аппаратной конфигурации, вы можете использовать один из нескольких методов. Шифрование BitLocker поддерживает пять режимов проверки подлинности в зависимости от аппаратных возможностей компьютера и требуемого уровня безопасности. Если аппаратная конфигурация поддерживает технологию доверенного платформенного модуля (TPM), то вы можете сохранять VMK как только в TMP, так и в TPM и на устройстве USB или сохранять ключ VMK в TPM и при загрузке системы вводить PIN. Помимо этого у вас есть возможность скомбинировать два предыдущих метода. А для платформ, которые не совместимы с технологией TPM, вы можете хранить ключ на внешнем USB устройстве.

Стоит обратить внимание на то, что при загрузке операционной системы с включенным шифрованием BitLocker, выполняется последовательность действий, которая зависит от набора средств защиты тома. Эти действия включают в себя проверку целостности системы, а также другие шаги по проверке подлинности, которые должны быть выполнены перед снятием блокировки с защищённого тома. В следующей таблице обобщены различные способы, которые вы можете использовать для шифрования тома:



Перед тем как BitLocker предоставит доступ к FEVK и расшифрует том, вам нужно предоставить ключи авторизированного пользователя или компьютера. Как было указано выше, если в вашем компьютере присутствует модуль TPM, вы можете использовать разные методы проверки аутентификации.

Использование только TPM

Процесс загрузки операционной системы использует TPM для того чтобы убедиться, что жесткий диск подключен к соответствующему компьютеру и важные системные файлы не были повреждены, а также предотвращает доступ к жесткому диску, если вредоносная программа или руткит поставил под угрозу целостность системы. В то время, когда компьютер проходит валидацию, TPM разблокирует VMK и ваша операционная система запускается без участия пользователя, как вы можете увидеть на следующей иллюстрации.

Использование TPM совместно с USB-ключом

В дополнение к физической защите, которая была описана в предыдущем подразделе, в этом случае TPM требует внешний ключ, который находится на USB-устройстве. В этом случае пользователю нужно вставить USB-накопитель, на котором хранится внешний ключ, предназначенный для аутентификации пользователя и целостности компьютера. В этом случае, вы можете защитить свой компьютер от кражи, при включении компьютера, а также при выводе из режима гибернации. К сожалению, этот способ не защитит вас от вывода компьютера из спящего режима. При использовании этого способа, для уменьшения риска при краже компьютера, вам нужно хранить внешний ключ отдельно от своего компьютера. На следующей иллюстрации вы можете ознакомиться с использованием TPM совместно с внешним USB-ключом:

Использование TPM совместно с PIN-кодом

Этот способ препятствует запуску компьютера до тех пор, пока пользователь не введет персональный идентификационный номер (PIN-код). Этот способ позволяет защитить ваш компьютер в том случае, если у вас был украден выключенный компьютер. К сожалению, вам не стоит использовать данный метод в том случае, если компьютер должен запускаться автоматически без участия человека, которые обычно выступают в качестве серверов. Когда запрашивается PIN, аппаратный модуль TPM компьютера отображает запрос для ввода четырехзначного PIN-кода со специальной задержкой, которая устанавливается производителями материнской платы и самого модуля TPM. На следующей иллюстрации вы можете увидеть данный способ проверки подлинности:

Использование комбинированного метода (TPM+PIN-код+USB-ключ)

В операционных системах Windows 7 и Windows Vista вы можете использовать комбинированный метод проверки подлинности для максимального уровня защиты вашего компьютера. В этом случае, к аппаратной проверке подлинности TPM добавляется ввод PIN-кода и использование внешнего ключа, который находится на USB-накопителе. Все эти средства обеспечивают максимальный уровень защиты BitLocker, которые требуют данные, которые «знает» и «использует» пользователь. Для того чтобы злоумышленник завладел вашими данными, которые расположены на защищённом при помощи технологии BitLocker томе, ему нужно украсть ваш компьютер, иметь в наличии USB-накопитель с вашим ключом, а также знать PIN-код, что

практически невозможно. На следующей иллюстрации изображен данный метод проверки подлинности:

Проверка подлинности только с USB-ключом запуска

В этом случае пользователь предоставляет VMK на диске, USB-накопителе или на любых внешних устройствах хранения данных для расшифровки FEVK и тома, зашифрованных при помощи технологии BitLocker на компьютере, в котором не установлен модуль TPM. Использование ключа запуска без TPM позволяет вам шифровать данные без обновления вашего аппаратного оборудования. Этот способ считается наиболее уязвимым, так как в этом случае нет проверки целостности и перенося жесткий диск на другой компьютер данными можно будет воспользоваться.

2.4.1. Использование BitLocker

При помощи технологии BitLocker вам предоставляется возможность зашифровать полностью весь диск, в то время как шифрованная файловая система (Encrypting File System, EFS) позволяет зашифровать лишь отдельные файлы. Технологие BitLocker обеспечивает шифрование «на лету», то есть, если на компьютере с зашифрованными файлами при помощи технологии BitLocker будет предоставлен общий доступ, то авторизованные пользователи смогут взаимодействовать с такими файлами также просто, как если бы никакого шифрования на компьютере такого пользователя не было. Помимо этого, в том случае, если файлы, расположенные на зашифрованном диске будут скопированы на другой компьютер или на незашифрованный диск, то тогда эти файлы будут автоматически расшифрованы.

Далее предложена инструкция для шифрования системного и дополнительных разделов на ноутбуке, не поддерживающем модуль TPM, с операционной системой Windows 7.

Включение шифрования BitLocker для системного раздела

Для того чтобы зашифровать системный раздел, выполните следующие действия:

1. Прежде всего, так как на ноутбуке, указанном в этом примере, на котором будут шифроваться диски, отсутствует доверенный платформенный модуль, желательно выполнить некоторые предварительные действия. Вам нужно открыть оснастку «Редактор локальной групповой политики» и перейти к узлу:

Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Шифрование диска BitLocker\Диски операционной системы

Здесь вы можете обнаружить шесть различных параметров политики. Так как было упомянуто ранее, что данный ноутбук не оснащён модулем TPM, нужно сделать так, чтобы перед загрузкой операционной системы, использовался USB-накопитель, содержащий специальный ключ, предназначенный для подтверждения проверки подлинности и последующей загрузки системы. Для выполнения этой операции предназначен параметр политики «Обязательная дополнительная проверка подлинности при запуске». В диалоговом окне свойств данного параметра политики вам следует установить флажок на опции «Разрешить использование BitLocker без совместимого TPM», затем сохраните выполненные изменения.

Для управления технологией BitLocker доступно много различных параметров групповой политики.

2. Откройте «Панель управления», перейдите к категории «Система и безопасность», а затем выберите «Шифрование диска BitLocker»;

3. В отобразившемся окне панели управления выберите системный раздел, а затем нажмите на ссылку «Включить BitLocker». Стоит обязательно обратить внимание на то, что вы сможете зашифровать раздел только в том случае, если он расположен на базовом диске. В том случае, если у вас созданы разделы на динамическом диске, перед их шифрованием вам нужно будет сконвертировать диск из динамического в базовый.

4. После выполнения проверки конфигурации компьютера, на первой странице мастера шифрования диска BitLocker вы можете указать различные параметры запуска. Но так как на моем ноутбуке нет доверенного платформенного модуля, а также был изменен параметр групповой политики, разрешающий использовать шифрование BitLocker на оборудовании без поддержки TPM, можно выбрать лишь параметр «Запрашивать ключ при запуске».

5. На странице «Сохраните ключ запуска» мастера шифрования диска BitLocker вам следует присоединить к компьютеру флэш-накопитель, а затем указать его в списке. После того как вы выберите накопитель, нажмите на кнопку «Сохранить»;

6. На третьей странице мастера вам предстоит указать расположение для ключа восстановления. Ключ восстановления представляет собой маленький текстовый файл, содержащий некоторые инструкции, метку диска, идентификатор пароля, а также 48-значный ключ восстановления. Необходимо помнить, что этот ключ отличается от ключа запуска тем, что он используется для получения доступа к

данным в тех случаях, когда невозможно получить к ним доступ любыми другими способами. Вы можете выбрать один из трех следующих вариантов: сохранить ключ восстановления на флэш-накопителе USB, сохранить ключ восстановления в файле или напечатать ключ восстановления. Учтите, что при выборе первого варианта, вам необходимо сохранять ключи восстановления и запуска на разных флэш накопителях. Если вы распечатываете ключ восстановления, то в этом случае корпорация Microsoft советует такой документ хранить в закрытом сейфе.

7. На последней странице мастера шифрования диска вы можете выполнить проверку системы BitLocker, при помощи которой убедитесь, что в случае необходимости будет предоставлена возможность с легкостью использовать свой ключ восстановления. Для завершения выполнения проверки системы вам будет предложено перезагрузить компьютер.

8. Сразу после POST-теста для запуска операционной системы вам будет предложно вставить флэш-накопитель с ключом запуска. После того как компьютер будет перезагружен и BitLocker-у будет известно, что после шифрования не случится никаких непредвиденных обстоятельств, начнется сам процесс шифрования диска. Об этом вы узнаете из значка, отображаемого в области уведомлений, или если перейдете к окну «Шифрование диска BitLocker» из панели управления. Сам процесс шифрования выполняется в фоновом режиме, то есть, вы во время выполнения шифрования сможете продолжить работу на компьютере, однако BitLocker будет интенсивно использовать ресурсы процессора и свободное место на шифруемом диске.

9. После завершения процесса шифрования диска BitLocker, вы будете уведомлены о том, что шифрование диска успешно завершено. В проводнике Windows на значке зашифрованного раздела изображается замок.

Шифрование USB-накопителей средствами групповой политики

Из следующей, несложной процедуры, вы узнаете о том, какие же действия следует выполнять для того, чтобы немного повысить безопасность вашего парка компьютеров от небрежного отношения пользователей к своим съемным устройствам. Другими словами, в данном разделе будут описаны действия, после которых будет выполнено шифрование BitLocker для USB-накопителей, которыми могут пользоваться ваши пользователи. Настройки шифрования USB-накопителей можно задать как для отдельного пользователя на локальном компью-

тере из рабочей группы, так и для подразделений или всех компьютеров домена при помощи функциональных возможностей групповой политики. Соответственно, чтобы зашифровать USB-накопитель, требуется выполнить следующие действия:

1. Для начала откройте оснастку «Управление групповой политикой». В дереве оснастки разверните узел «Лес: %имя леса%», узел «Домены», затем узел с именем вашего домена, а после этого перейдите к контейнеру «Объекты групповой политики». В выбранном контейнере «Объекты групповой политики» создайте объект групповой политики, например, «Политика для шифрования съемных дисков компании». После этого выберите созданный только что объект GPO, нажмите на нем правой кнопкой мыши и из контекстного меню выберите команду «Изменить»;

2. В отобразившейся оснастке «Редактор управления групповой политики» перейдите к узлу

Конфигурация компьютера\Политики\Административные шаблоны\Компоненты Windows\Шифрование диска BitLocker

и выберите узел«Съемные диски с данными». Перейдя к данному узлу, здесь можно обнаружить шесть параметров политики.

Первый параметр предназначен для управления возможностью настройки BitLocker пользователями, соответственно для своих USB-накопителей на своих компьютерах. Для этого следует открыть диалоговое окно свойств параметра политики «Управление использованием BitLocker для съемных носителей». Здесь, помимо опции «Включить», переключатель на которую обязательно будет установлен, еще присутствуют два управляющих элемента. Первый контрол, у которого вы можете установить флажок, называется «Разрешить пользователям применять защиту BitLocker для съемных дисков с данными» позволяет пользователям самостоятельно запускать мастер шифрования BitLocker и зашифровывать свои съемные носители. Ну а если вы установите флажок на опции «Разрешить пользователям временно приостанавливать защиту BitLocker и расшифровывать съемные диски с данными», вы тем самым разрешите пользователям отключать шифрование для своих накопителей.

3. Теперь, после того как пользователи смогут самостоятельно шифровать свои USB-накопители, мы можем им запретить на своих компьютерах использовать флэшки в качестве устройств, предназначенных для записи, которые еще не были зашифрованы при помощи технологии BitLocker. Другими словами, используя возможности параметра политики «Запретить запись на съемные диски, не защи-

щенные BitLocker», USB-накопители, которые не были зашифрованы, могут использоваться лишь в качестве устройства, предназначенного только для чтения. В том случае, если вы установите флажок на опции «Запретить запись на устройства, настроенные в другой организации», запись на USB-накопитель будет разрешена лишь в том случае, если поля идентификации на дисках совпадают с полями идентификации компьютера пользователя. Идентификаторы можно настраивать для устройства при помощи утилиты командной строки Manage-bde. В данном примере не будет устанавливаться этот флажок, а просто сохраним изменения с установленным переключателем на опции «Включить»;

4. Какова вероятность, что пользователь со своей флэшкой придет домой, а у него там установлена операционная система Windows 7? Может у пользователя очень старый компьютер и там установлена система Windows XP. В таком случае, чтобы пользователь смог там использовать свой USB-накопитель, следует настроить BitLocker To Go. Используя параметр политики «Разрешить доступ к съемным дискам с данными, защищенным с помощью BitLocker, из более ранних версий Windows» вы можете указать, что съемные накопители, которые отформатированы в файловой системе FAT можно будет использовать в устаревших операционных системах. Если параметр политики включен, и вы не установили флажок на опции «Не устанавливать BitLocker To Go Reader на съемных дисках, отформатированных с системой FAT», то на клиентские компьютеры при установке флэшки будет устанавливаться программа bitlockertogo.exe.

5. Как можно сделать USB-накопитель еще безопаснее? Конечно, для этого следует в дополнение к шифрованию еще задать пароль, предназначенный для выполнения расшифровки информации. И эту возможность также вы можете задать при помощи функциональных возможностей групповой политики. Для этого откройте диалоговое окно свойств параметра политики «Настроить использование паролей для съемных дисков с данными» и установите переключатель на опцию «Включить». Помимо этого, установив флажок возле опции «Требовать пароль для съемного диска с данными», вы тем самым укажите, что это требование является обязательным, и вы не сможете использовать свой накопитель, если для него не будет указан пароль. Здесь же вам предоставляется возможность определения минимальной длины пароля, а также уровень его сложности.

2.5. Авторизация

Авторизация — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий. Часто можно услышать выражение, что какой-то человек «авторизован» для выполнения данной операции — это значит, что он имеет на неё право.

Авторизацию не следует путать с аутентификацией: аутентификация — это лишь процедура проверки подлинности данных, например, проверки соответствия введённого пользователем пароля к учётной записи паролю в базе данных, или проверка цифровой подписи письма по ключу шифрования, или проверка контрольной суммы файла на соответствие заявленной автором этого файла. Другими словами, авторизация подразумевает идентификацию и аутентификацию.

Сегодня проблемы авторизации в Windows сложно назвать надуманными. К аутентификации по паролю предъявляются все более сложные требования. Пароль длиной в восемь символов, содержащий три набора из четырех, уже не является настолько устойчивым к взлому, как два-три года назад. А если вы поставите длину пароля еще больше, пользователи начнут записывать их на бумаге и приклеивать к монитору.

В следующей таблице представлена оценка времени взлома пароля путем перебора. Данные рассчитаны исходя из вычислительной мощности, доступной взломщику на 2013 год.

Набор символов	Число символов	длина пароля – 7 символов	длина пароля – 8 символов
Цифры	10	0	0,0001
Маленькие (большие) буквы	26	0,064	0,1664
Цифры и маленькие буквы	36	0,0624	2,248
Цифры, маленькие и большие буквы	62	2,8062	173,9838
Цифры, маленькие и большие буквы и спецсимволы	72	7,9929	575,4866

Если считать, что на предприятии установленное время жизни пароля – 42 дня, как это рекомендовано Microsoft, то несложно оценить вероятность взлома пароля за этот период:

Набор символов	Число символов	длина пароля – 7 символов	длина пароля – 8 символов
Цифры	10	100%	100%

Маленькие (большие) буквы	26	100%	100%
Цифры и маленькие буквы	36	100%	100%
Цифры, маленькие и большие буквы	62	100%	24,14%
Цифры, маленькие и большие буквы и спец-символы	72	100%	7,30%

Для подобных атак наиболее успешно применяются ботнеты: в этом случае, если злоумышленнику удастся обойти систему защиты от перебора (например, получить хэш пароля или часть информации, зашифрованной с помощью этого пароля), то скорость перебора будет зависеть только от размера сети зараженных компьютеров.

Наиболее распространенный выход из данной ситуации – применение аппаратной аутентификации на базе электронных токенов. Кроме того, сегодня на рынок средств аутентификации все чаще выходят средства биометрической аутентификации.

2.5.1. Токен авторизации

В контексте информационной безопасности токен — это компактное устройство, которое служит для авторизации пользователя, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения любых персональных данных; также называется «ключ». Как правило, это физическое устройство, используемое для упрощения аутентификации. Также этот термин может относится и к программным токенам, которые выдаются пользователю после успешной авторизации и являются ключом для доступа к службам.

Токены предназначены для электронного удостоверения личности (например, клиента, получающего доступ к банковскому счёту), при этом они могут использоваться как вместо, так и вместе с паролем. В некотором смысле токен — это электронный ключ для доступа к чему-либо.

Обычно аппаратные токены обладают небольшими размерами, что позволяет носить их в кармане или кошельке, часто они выглядят в виде брелоков. Некоторые предназначены для хранения криптографических ключей, таких как электронная подпись или биометрические данные (например, детали дактилоскопического узора). В одни встроена защита от взлома, в другие — мини-клавиатура для ввода PIN-кода или же просто кнопка вызова процедуры генерации и дисплей для вывода сгенерированного ключа. Токены обладают разъёмом USB, функ-

циями RFID или беспроводным интерфейсом Bluetooth для передачи сгенерированной последовательности ключей на клиентскую систему.

Все токены содержат некоторые секретные сведения, которые используются для подтверждения личности. Есть четыре различных способа, в которых эта информация может быть использована:

Токен со статическим паролем.

Устройство содержит пароль, который физически скрыт (не виден обладателю), но который передается для каждой аутентификации. Этот тип уязвим для атак повторного воспроизведения.

Токен с синхронно динамическим паролем.

Устройство генерирует новый уникальный пароль с определенным интервалом времени. Токен и сервер должны быть синхронизированы, чтобы пароль был успешно принят.

Токен с асинхронным паролем.

Одноразовый пароль генерируется без использования часов, с помощью шифра Вернама или другого криптографического алгоритма.

Токен вызов-ответ.

Используя криптографию с открытым ключом, можно доказать владение частным ключом, не раскрывая его. Сервер аутентификации шифрует вызов (обычно случайное число или по крайней мере, данные с некоторыми случайными частями) с помощью открытого ключа. Устройство доказывает, что обладает копией соответствующего частного ключа, путем предоставления расшифрованного вызова.

Одноразовые пароли, синхронизированные по времени

Синхронизированные по времени одноразовые пароли постоянно меняются в установленное время, например, раз в минуту. Для этого должна существовать синхронизация между токеном клиента и сервером аутентификации. Для устройств не подключенных к сети, эта синхронизация сделана до того, как клиент приобрел токен. Другие типы токенов синхронизируются, когда токен вставляется в устройство ввода. Главная проблема с синхронизированными токенами состоит в том, что они могут рассинхронизоваться, спустя какой-то большой период времени. Тем не менее, некоторые системы, такие как SecurID компании RSA, позволяют пользователю синхронизировать сервер с токеном, путем ввода нескольких последовательных кодов доступа. Большин-

ство из них не может иметь сменные батареи, следовательно имеют ограниченный срок службы.

Одноразовые пароли на основе математического алгоритма

Другой тип одноразовых паролей использует сложный математический алгоритм, например, хэш-цепи, для создания серии одноразовых паролей из секретного ключа. Ни один из паролей нельзя отгадать, даже тогда, когда предыдущие пароли известны. Существует общедоступный, стандартизированный алгоритм OATH (Initiative For Open Authentication); другие алгоритмы покрыты американскими патентами. Каждый новый пароль должен быть уникальным, поэтому неавторизованный пользователь не сможет догадаться, что новый пароль может быть, на основе ранее использованных паролей.

Уязвимости токенов авторизации

Самая простейшая уязвимость с любым токеном - это его потеря или кража. Вероятность случая компрометации может быть уменьшена с помощью личной безопасности, например: замки, электронная привязь, сигнализация. Украденные токены - бесполезны для вора, если использована технология двухфакторной аутентификации. Как правило для проверки подлинности требуется вводить персональный идентификационный номер (PIN) вместе с информацией на токене.

Любая система, которая позволяет пользователям аутентифицироваться через ненадежную сеть (например, Интернет) является уязвимой к MITM-атаке (англ. Man in the middle, “человек посередине”).

2.5.2. Биоэлектронные системы авторизации

Как правило, для защиты компьютерных систем от несанкционированного доступа применяется комбинация из двух систем – биометрической и контактной на базе смарт-карт или USB-ключей. Что скрывается за понятием «биометрия»? Фактически мы используем эти технологии каждый день, однако это понятие как технический способ аутентификации появилось относительно недавно. Биометрия – это идентификация пользователя по уникальным, присущим только данному пользователю, биологическим признакам. Такие системы являются самыми удобными, с точки зрения самих пользователей, так как им не приходится ничего запоминать и такие характеристики весьма сложно потерять. При биометрической идентификации в базе данных хранится цифровой код, ассоциированный с определенным человеком. Сканер или другое устройство, используемое для аутентификации,

считывает определенный биологический параметр. Далее он обрабатывается по определенным алгоритмам и сравнивается с кодом. Просто? С точки зрения пользователя – безусловно. Однако у данного метода существуют и свои недостатки.

К достоинствам биометрических сканеров обычно относят то, что они никак не зависят от пользователя (например, можно ошибиться при вводе пароля) и никто не может передать свой биологический идентификатор другому человеку, в отличие от пароля. Однако, как показали проведенные в США исследования, биометрические сканеры, основанные на отпечатках пальцев, довольно легко обмануть с помощью муляжа. Или ситуация с отказом в доступе, осуществляемом на основании распознавания голоса, в случае если человек простужен.

К биометрическим относятся различные методы. Все их можно разбить на две подгруппы:

статические методы, которые основываются на физиологической (статической) характеристике человека, то есть уникальном свойстве, данном ему от рождения и неотъемлемом от него. К статическим относятся форма ладони, отпечатки пальцев, радужная оболочка, сетчатка глаза, форма лица, расположение вен на кисти руки и т. д.;

динамические методы, которые основываются на поведенческой (динамической) характеристике человека – особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия (подписи, речи, динамики клавиатурного набора).

Методы формирования и применения биометрических характеристик в целях идентификации или верификации личности называются биометрическими технологиями (БТ). В БТ используются как статические, так и динамические источники биометрических характеристик. В основном в настоящее время предлагается использовать следующие источникам статических биометрических характеристик:

• Форма лица (овал, форма и размер отдельных деталей лица)
• Геометрические параметры лица – расстояния между его определенными точками
• Узор подкожных кровеносных сосудов на термограмме лица
• Структура радужной оболочки глаза
• Узор кровеносных сосудов на сетчатке
• Форма уха (контур и наклон, козелок и противокозелок. форма и прикрепление мочки и т.д.)

• Геометрические параметры уха – расстояния между определенными точками на ухе
• Геометрия руки – ширина, длина, высота пальцев, расстояния между определенными точками
• Неровности складок кожи на сгибах пальцев тыльной стороны кисти руки
• Рисунок вен на тыльной стороне кисти руки, получаемый при инфракрасной подсветке
• Узор на ладони. Папиллярный узор как целостный образ
• Параметры минуций (координаты, ориентация, тип)
• Параметры пространственно-частотного спектра папиллярного узора
• Подпись как двухмерный бинарный образ
• Подпись как функция двух координат
• Динамика подписи (сила нажима и координата времени)

Идеальная биометрическая характеристика человека (БХЧ) должна быть универсальной, уникальной, стабильной, собираемой. Универсальность означает наличие биометрической характеристики у каждого человека. Уникальность означает, что не может быть двух человек, имеющих идентичные значения БХЧ. Стабильность – независимость БХЧ от времени. Собираемость – возможность получения биометрической характеристики от каждого человека.

Реальные БХЧ не идеальны и это ограничивает их применение. В результате экспертной оценки указанных свойств таких источников БХЧ, как изображения и термограммы лица, отпечатков пальцев, геометрии руки, радужной оболочки глаза (РОГ), изображения сетчатки, подписи, голоса, изображения губ, ушей, динамики почерка и походки, установлено, что ни одна из характеристик не удовлетворяет требованиям по перечисленным свойствам. Необходимым условием использования тех или иных БХЧ является их универсальность и уникальность, что косвенно может быть обосновано их взаимосвязью с генотипом или кариотипом человека.

В следующей таблице приведена экспертная оценка свойств БХЧ.

Источник БЧХ	Универсальность	Уникальность	Стабильность	Собираемость
Видеообраз лица	+++	+	++	+++
Термограмма лица	+++	+++	+	++
Отпечаток пальца	+++	+++	+++	++
Форма руки	++	++	++	+++

РОГ	++	+++	+++	++
Сетчатка	+++	+++	++	+
Подпись	+	+	+	+++
Голос	++	+	+	++
Губы	+++	+++	++	+
Уши	++	++	++	++
Динамика письма	++	+++	+	+++
Походка	+++	++	+	+

Здесь (+++) – высокая оценка. (++) – средняя, (+) – низкая.

Распознавание по отпечаткам пальцев

Распознавание по отпечаткам пальцев – самый распространенный статический метод биометрической идентификации, в основе которого лежит уникальность для каждого человека рисунка папиллярных узоров на пальцах. Изображение отпечатка пальца, полученное с помощью специального сканера, преобразуется в цифровой код (свертку) и сравнивается с ранее введенным шаблоном (эталоном) или набором шаблонов (в случае аутентификации).

Распознавание по форме руки

Данный статический метод построен на распознавании геометрии кисти руки, также являющейся уникальной биометрической характеристикой человека. С помощью специального устройства, позволяющего получать трехмерный образ кисти руки (некоторые производители сканируют форму нескольких пальцев), получаются измерения, необходимые для получения уникальной цифровой свертки, идентифицирующей человека.

Распознавание по радужной оболочке глаза

Этот метод распознавания основан на уникальности рисунка радужной оболочки глаза. Для реализации метода необходима камера, позволяющая получить изображение глаза человека с достаточным разрешением, и специализированное программное обеспечение, позволяющее выделить из полученного изображения рисунок радужной оболочки глаза, по которому строится цифровой код для идентификации человека.

Распознавание по форме лица

В данном статическом методе идентификации строится двух- или трехмерный образ лица человека. С помощью камеры и специализированного программного обеспечения на изображении или наборе изображений лица выделяются контуры бровей, глаз, носа, губ и т. д., вычисляются расстояния между ними и другие параметры, в зависимости от используемого алгоритма. По этим данным строится образ, выраженный в цифровой форме для сравнения. Причем количество, качество и разнообразие (разные углы поворота головы, изменения нижней части лица при произношении ключевого слова и т. д.) считываемых образов может варьироваться в зависимости от алгоритмов и функций системы, реализующей данный метод. К динамическим относят те характеристики, которые могут меняться со временем. Это такие параметры, как почерк, подпись, голос и т. д.

Распознавание по рукописному почерку

Как правило, для этого динамического метода идентификации человека используется его подпись (иногда написание кодового слова). Цифровой код идентификации формируется по динамическим характеристикам написания, то есть для идентификации строится свертка, в которую входит информация по графическим параметрам подписи, временным характеристикам нанесения подписи и динамики нажима на поверхность в зависимости от возможностей оборудования (графический планшет, экран карманного компьютера и т. д.).

Распознавание по клавиатурному почерку

Метод в целом подобен описанному выше, однако вместо подписи в нем используется некое кодовое слово, а из оборудования требуется только стандартная клавиатура. Основная характеристика, по которой строится свертка для идентификации, – динамика набора кодового слова.

Распознавание по голосу

В настоящее время развитие этой одной из старейших технологий ускорилось, так как предполагается ее широкое использование при сооружении интеллектуальных зданий. Существует достаточно много способов построения кода идентификации по голосу: как правило, это различные сочетания частотных и статических его характеристик. Однако стоит учесть, что идентификация по статическим характеристикам более надежна, так как не зависит от психоэмоционального состояния человека.

Помимо перечисленных производителей сейчас на рынке биометрии появилась новая группа компаний, чьи решения называются промежуточными. Как правило, это «программное обеспечение-посредник» между оконечным оборудованием и программными системами, в которые интегрируются процедуры биометрической идентификации. Причем посредник может реализовать как просто регистрацию в системе с использованием измерений биометрического сканера (например, Windows Logon), так и самостоятельные функции, например создание криптографических контейнеров с помощью ключа, получаемого только по определенному отпечатку пальца.

Недостатки

К недостаткам биометрической аутентификации стоит отнести следующие. Прежде всего, это недостатки самих биометрических сканеров. Например, сканеры отпечатков пальцев могут быть оптическими и электронными. Первые обеспечивают более качественное изображение, однако быстрее загрязняются и более требовательны к чистоте рук. Вторые – менее надежные и качественные, зато могут распознавать отпечатки не слишком чистых пальцев.

Второй недостаток – это крайне сложная корректная настройка оборудования, вернее, речь идет об установке корректного порогового значения ошибки. FAR (False Acceptance Rate) – вероятность допуска в системунезарегистрированного человека, FRR (False Rejection Rate) – это процент ложных отказов в допуске. Порог чувствительности является своеобразной гранью идентификации. Человек, имеющий сходство какой-либо характеристики выше предельного, будет допущен в систему, и наоборот. Значение порога администратор может изменять по своему усмотрению. Таким образом, это накладывает определенные обязательства на администратора системы, ведь обеспечение баланса между удобством и надежностью требует больших усилий.

Третьим недостатком, связанным с внедрением таких систем, является недовольство сотрудников компаний, связанное с возможностью контроля рабочего времени. Тем более что системы учета рабочего времени сотрудников все равно существуют.

Биометрические сканеры невозможно применять для идентификации людей с некоторыми физическими недостатками, как утверждает профессор антропологии Университетского колледжа Лондона Анжела Сесс. Так, применение сканеров сетчатки глаза будет сложным для тех, кто носит очки или контактные линзы, а человек, больной

артритом, не сможет ровно положить палец на сканер отпечатка. Еще одна проблема – рост. Сканирование лица может оказаться затруднительным, если рост человека ниже 1,55 м или выше 2,1 м. Преступники, по словам профессора Сесс, смогут легко обмануть биометрические системы. К недостаткам такого способа идентификации можно еще отнести возможность воспользоваться муляжом отпечатка, что было успешно продемонстрировано заключенными шотландской тюрьмы строгого режима Glenochil.

Биометрия в Windows 7

В состав Windows 7 входит биометрическая платформа Windows – Windows Biometric Framework, которая обеспечивает единообразное представление сканеров отпечатков пальцев и других биометрических устройств в форме, удобной высокоуровневым приложениям, а также позволяет единообразно использовать приложения для анализа отпечатков пальцев. В предыдущих версиях Windows сканеры отпечатков пальцев поддерживались как средство регистрации в системе. Такими сканерами сейчас оборудованы многие переносные компьютеры, но для их работы были необходимы драйверы и специальное программное обеспечение. Теперь поддержка таких устройств является частью Windows 7, и для их работы ничего, кроме драйвера, не требуется.

Анализ мер по снижению риска биометрической аутентификации

Если на предприятии вместе с Windows 7 планируется внедрение биометрического механизма проверки, например сканирования отпечатков пальцев, следует заранее учесть следующие соображения.

Биометрические системы обычно требуют хранения на компьютере информации, которая может использоваться для установления личности. По этой причине предприятию придется заниматься обеспечением конфиденциальности.

Многие современные переносные компьютеры обладают встроенными сканерами отпечатков пальцев, что может упростить внедрение биометрического решения, однако по функциональности и качеству распознавания такие встроенные устройства уступают специализированному оборудованию. Следует сравнить относительное качество по таким показателям, как коэффициент ложного пропуска, коэффициент ложного отказа, коэффициент ошибок кроссовера, коэффициент ошибок регистрации и пропускная способность.

Если по характеру работы пользователи или компьютеры оказываются в загрязненных помещениях, где сложно поддерживать чистоту рук или требуются перчатки, сканеры отпечатков использовать не удастся. Эту проблему можно решить за счет систем анализа других физиологических параметров, например геометрии лица, радужной оболочки глаза или ладони.

Наряду с биометрическим подтверждением пользователю необходимо предоставлять какое-либо иное свидетельство, например ключевую фразу, PIN-код или смарт-карту, поскольку биометрические устройства можно обмануть.

Процесс снижения рисков

Особенности внедрения биометрических средств на каждом предприятии свои. Однако общую последовательность действий определить можно.

Установить, какие из имеющихся механизмов проверки биометрических данных больше подходят нуждам предприятия.

Проанализировать внутреннюю документацию по обеспечению конфиденциальности, чтобы убедиться в возможности управления конфиденциальными биометрическими данными.

Определить требования к оборудованию, используемому при биометрическом сканировании, и наметить сроки выполнения этих требований.

Определить элементы инфраструктуры, необходимые для биометрического сканирования, такие как инфраструктура публичных ключей или требования к клиентскому программному обеспечению.

Установить, у каких сотрудников могут возникнуть проблемы с использованием биометрической системы, и подобрать для них альтернативные варианты, например проверку по имени пользователя и паролю или смарт-карте с PIN-кодом.

Заранее обучить пользователей обращению с системой биометрической проверки подлинности, а тех, кто не сможет ею пользоваться, – альтернативным методам проверки.

Провести масштабный пробный запуск в целях выявления и разрешения проблем до начала повсеместного внедрения.

Следуя инструкциям производителя по сканированию и проверке, ввести данные о пользователях в биометрическую систему.

Обучить пользователей обращению с системой, обеспечить помощь для тех, кто испытывает трудности.

Необходимо учесть, что некоторые пользователи могут категорически отказаться применять биометрическую систему. Для таких пользователей следует предусмотреть альтернативный способ проверки подлинности.

Использование групповой политики для снижения рисков, связанных с биометрической проверкой

Доступные в данной категории параметры находятся в разделе редактора групповых политик Конфигурация компьютера>Административные шаблоны>Компоненты Windows>Биометрия.

В следующей таблице приведены параметры этой технологии, применимые к Windows 7.

Объект политики	Описание	По умолч. в Windows 7
Разрешить использование биометрии	Если данный параметр включен или не задан, то разрешается запуск приложений, использующих средства Windows по проверке биометрии	Не задано
Разрешить пользователям выполнять регистрацию в системе с использованием биометрии	Этот параметр политики определяет, можно ли пользователям осуществлять регистрацию в системе или производить повышение прав с помощью биометрии. По умолчанию локальным пользователям разрешена регистрация в системе локального компьютера	Не задано
Разрешить пользователям домена выполнять регистрацию в системе с использованием биометрии	Этот параметр политики определяет, можно ли пользователям домена осуществлять регистрацию в системе или производить повышение прав с помощью биометрии. По умолчанию пользователи домена не могут использовать такой способ регистрации в системе	Не задано
Время ожидания для событий функции быстрого переключения пользователей	Этот параметр политики задает количество секунд (до 60 максимум), в течение которого остается активным событие быстрого переключения пользователей, перед тем как переключение произойдет. По умолчанию событие быстрого переключения остается активным 10 секунд, затем переходит в неактивное состояние	Не задано

ГЛАВА 3. БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СЕТИ

В данной главе описаны термины, понимание которых необходимо при использовании сетевой передачи данных на защищенном компьютере.

Так как сетевая безопасность – это обширная область знаний, понимание которой требует навыков администрирования сети, в данном пособии эти вопросы признаются отдельной темой и не рассматриваются. Обратите внимание, что изложенные в данной главе рекомендации помогут обеспечить безопасность только при использовании безопасной сети и при условии, что операционная система защищена должным образом.

Не следует подключать компьютер к небезопасной сети (например, практически все домашние провайдеры не обеспечивают достаточной защиты). Всегда используйте соединения с надёжным шифрованием при передаче конфиденциальной информации.

3.1. Цифровые сертификаты

Существует два основных класса криптографических алгоритмов – симметричные и ассиметричные. В симметричных для шифрования и дешифрования сообщения используется один и тот же ключ. В ассиметричных разные. Тот, которым расшифровывают сообщения, называется закрытым ключем, ключ для шифрования называется открытым. Поэтому раздел криптографии изучающий свойства открытых ключей получил название криптография открытого ключа. С помощью открытых и закрытых ключей можно подписывать документы. Для этого рядом с ключем сохраняют данные о владельце ключа и полученный файлы называется сертификатом. Вся система взаимотношений между владельцами сертификатов построена на доверии к определенным пользователям. Их подписи общеизвестны, и они подписывают сертификаты других членов, подтверждая тем самым достоверность открытого ключа и хранящихся вместе с ним данных о владельце. Для того что бы система не была скомпрометирована, пользователи принимают только сертификаты с подписями доверенных членов. Приведем более строгую терминологию:

Инфраструктура открытого ключа (PKI) является системой цифровых сертификатов, центров сертификации (ЦС), которая производит проверку и подтверждение подлинности каждой из сторон, участвующих в электронной операции, с помощью криптографии открытых ключей.

Сертификат открытого ключа, обычно называемый просто сертификатом - это документ с цифровой подписью, связывающий значение открытого ключа с удостоверением пользователя, устройства или службы, которым принадлежит соответствующий закрытый ключ.

Центр Сертификации (Certification Authority, CA, ЦС) является пакетом программного обеспечения, принимающим и обрабатывающим запросы на выдачу сертификатов, издающим сертификаты и управляющим выданными сертификатами.

Корневой сертификат - сертификат принадлежащий Центру Сертификации, с помощью которого проверяется достоверность других выданных центром сертификатов.

Список отозванных сертификатов - список скомпрометированных или недействительных по какой либо другой причине сертификатов.

Отличительное имя (Distinguished Name, DN) - данные о владельце сертификата. Включают CN (Common Name), OU (Organization Unit), O (Organization), L (Locality), ST (State or province), C (Country name).

Электронная цифровая подпись (ЭЦП)- реквизит электронного документа предназначенный для удостоверения источника данных и защиты данного электронного документа от подделки.

Схема электронной подписи обычно включает в себя:

алгоритм генерации ключей пользователя;

функцию вычисления подписи;

функцию проверки подписи.

Функция вычисления подписи на основе документа и секретного ключа пользователя вычисляет собственно подпись. Функция проверки подписи проверяет, соответствует ли данная подпись данному документу и открытому ключу пользователя. Открытый ключ пользователя доступен всем, так что любой может проверить подпись под данным документом.

Для того что бы подписать документ нужно зашифровать с помощью закрытого ключа значение хеш-функции от содержимого документа. Что бы проверить подпись, нужно расшифровать с помощью открытого ключа значение подписи и убедиться, что оно равно хешу подписанного документа. Таким образом цифровая подпись, это зашифрованный хеш документа.

Ключ - это набор параметров (чисел). Он может храниться в файле. В теории клиенты должны сами генерировать свои закрытые и открытые ключи, создавать запрос на подпись открытого ключа и от-

правлять его в центр. На практике большинство клиентов не умеют генерировать ключи, поэтому в нашем случае Центр осуществляет данную работу. Центр может отзывать сертификат, выданный клиенту, помещая его в черный список, который регулярно передается пользователям центра. С помощью корневого сертификата, который публично доступен, пользователи могут проверять сертификаты друг друга.

Итого у центра сертификации имеется:

- Закрытый ключ
- Корневой сертификат (хранящий в себе открытый ключ);
- Список отозванных (скомпрометированных) сертификатов

У клиентов:

- закрытый ключ;
- сертификат, подписанный корневым;
- корневой сертификат для проверки того, что сертификаты других пользователей выданы его доверенным центром;
- список отозванных (скомпрометированных) сертификатов.

Создание корневого сертификата включает:

- Генерацию закрытого ключа.
- Генерацию открытого ключа и его подпись с помощью закрытого.
- Создание обычного сертификата включает:
- Генерацию закрытого ключа.
- Создание запроса на подпись сертификата.
- Подпись запроса в центре сертификации о получение сертификата.

Общепринятый формат информации, содержащейся в сертификате, называется X509. Сертификаты и ключи могут храниться в разных типах файлов.

3.2. Защищенное гипертекстовое соединение (HTTPS)

HTTPS не является отдельным протоколом. Это обычный HTTP, работающий через шифрованные транспортные механизмы SSL и TLS. Он обеспечивает защиту от атак, основанных на прослушивании сетевого соединения — от снифферских атак и атак типа man-in-the-middle при условии, что будут использоваться шифрующие средства и сертификат сервера проверен и ему доверяют.

По умолчанию HTTPS URL использует 443 TCP-порт (для незащищённого HTTP — 80). Чтобы подготовить веб-сервер для обработки https-соединений, администратор должен получить и установить в систему сертификат для этого веб-сервера. Сертификат состоит из 2 частей (2 ключей) — public и private. Public-часть сертификата используется для зашифрования трафика при передаче данных от клиента к серверу в защищённом соединении, private-часть — для расшифрования полученного от клиента зашифрованного трафика на сервере. После того как пара ключей приватный/публичный сгенерированы, на основе публичного ключа формируется запрос на сертификат в Центр сертификации, в ответ на который ЦС высылает подписанный сертификат. ЦС при подписывании проверяет клиента, что позволяет ему гарантировать, что держатель сертификата является тем, за кого себя выдаёт (обычно это платная услуга).

Существует возможность создать такой сертификат, не обращаясь в ЦС. Такие сертификаты могут быть созданы для серверов, работающих под Unix, с помощью таких утилит, как ssl-ca от OpenSSL или gensslcert от SuSE. Подписываются такие сертификаты этим же сертификатом и называются самоподписанными (self-signed). Без проверки сертификата каким-то другим способом (например, звонок владельцу и проверка контрольной суммы сертификата) такое использование HTTPS подвержено MITM-атаке (человек посередине).

Эта система также может использоваться для аутентификации клиента, чтобы обеспечить доступ к серверу только авторизованным пользователям. Для этого администратор обычно создаёт сертификаты для каждого пользователя и загружает их в браузер каждого пользователя. Также будут приниматься все сертификаты, подписанные организациями, которым доверяет сервер. Такой сертификат обычно содержит имя и адрес электронной почты авторизованного пользователя, которые проверяются при каждом соединении, чтобы проверить личность пользователя без ввода пароля.

Сам факт использования SSL не означает безопасности. Убедитесь, что сервер, с которым вы работаете, использует технологии безопасности корректно.

3.3. Cookies

Ку́ки (от англ. cookie — печенье) — небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя. Веб-клиент (обычно веб-браузер) всякий раз при попытке открыть

страницу соответствующего сайта пересылает этот фрагмент данных веб-серверу в виде HTTP-запроса. Применяется для сохранения данных на стороне пользователя, на практике обычно используется для:

- аутентификации пользователя;
- хранения персональных предпочтений и настроек пользователя;
- отслеживания состояния сеанса доступа пользователя;
- ведения статистики о пользователях.

Приём браузерами куки требуют многие сайты с ограничениями доступа, большинство интернет-магазинов. Настройка оформления и поведения многих веб-сайтов по индивидуальным предпочтениям пользователя тоже основана на куки. С момента своего появления куки вызывали обеспокоенность пользователей Интернета, поскольку слежение за действиями и предпочтениями пользователей может подвергнуть опасности тайну личной жизни. Куки легко перехватить и подменить (например, для получения доступа к учетной записи), если пользователь использует нешифрованное соединение с сервером. В группе риска пользователи, выходящие в интернет при помощи публичных точек доступа Wi-Fi и не использующие при этом таких механизмов как SSL.

В контексте информационной безопасности рекомендуется не использовать куки, если в этом нет необходимости.

3.4. Уязвимые браузерные технологии.

Некоторые задачи требуют использования технологий, подразумевающих выполнение браузером программы, загружаемой из интернета. К таким технологиям можно отнести Javascript, ActiveX, Flash, апплет Java и др. Страницы из недостоверных источников не должны иметь разрешений для выполнения таких программ.

Как правило, права таких программ сильно ограничены, однако уязвимости в браузерах могут дать возможность атаковать посетителя сайта. Кроме того, вредоносный код может быть внедрен в запрашиваемую страницу с помощью MITM-атаки.

Разрешение использования всех браузерных технологий на любом сайте открывает широкие возможности по внедрению CSRF-атаки (англ. Cross Site Request Forgery — «Межсайтовая подделка запроса», также известен как XSRF): от лица, открывшего страницу в браузере тайно отправляется запрос на другой сервер (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию

(например, перевод денег на счёт злоумышленника). Для осуществления данной атаки, жертва должна быть авторизована на том сервере, на который отправляется запрос, и этот запрос не должен требовать какого-либо подтверждения со стороны пользователя, который не может быть проигнорирован или подделан атакующим скриптом.

3.5. Безопасность электронной почты

Сами по себе технологии, позволяющие получать и передавать почту не обеспечивают защиту информации. Например, повсеместно применяемый протокол отправки почты SMTP не проверяет адрес, который указывается в поле FROM (адрес отправителя). Это означает, что, как и по обычной почте, по электронной почте можно отправить письмо от имени другого человека (или организации).

Для защиты электронной почты применяется ассиметричное шифрование. Используйте цифровые подписи, чтобы подтверждать личность отправителя. Используйте шифрование сообщений (например, на основе PGP или GPG), если вы передаете по электронной почте конфиденциальную информацию.

ГЛАВА 4. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

4.1. Что такое Социальная инженерия

Для проведения атак злоумышленники, применяющие методы социотехники, эксплуатируют в своих целях доверчивость, лень, любезность и даже энтузиазм сотрудников организации. Защититься от таких атак непросто, поскольку их жертвы могут не подозревать, что их обманули, а даже если и подозревают, часто предпочитают не рассказывать об этом. Злоумышленники (люди, пытающиеся получить несанкционированный доступ к компьютерным системам), которые используют методы социотехники, преследуют, в общем, такие же цели, что и любые другие злоумышленники: им нужны деньги, информация или информационные ресурсы компании-жертвы.

Для этого злоумышленник, использующий методы социотехники, пытается убедить сотрудников компании предоставить ему информацию, обеспечивающую доступ к корпоративным системам или их ресурсам. Такой подход традиционно называют *злоупотреблением доверием*. Во многих компаниях малого и среднего размера считают, что для злоумышленников представляют интерес только крупные богатые корпорации. Возможно, раньше так и было, но нынешний рост кибер-

преступности свидетельствует о том, что теперь злоумышленники не гнушаются никакими способами получения выгоды, атакуя и крупные компании, и системы домашних пользователей. Злоумышленники могут красть средства или ресурсы непосредственно у атакуемой компании, но могут и использовать ее в качестве точки опоры для проведения атак на другие организации. Это осложняет расследование таких преступлений и поимку преступников.

Для защиты от атак, основанных на методах социотехники, нужно изучить их разновидности, понять, что нужно злоумышленнику, и оценить ущерб, который может быть причинен организации. Обладая этой информацией, можно интегрировать в политику безопасности меры защиты от атак, основанных на методах социотехники. В данном документе предполагается, что в организации принята политика безопасности, определяющая цели, методики и процедуры защиты корпоративных информационных активов, ресурсов и сотрудников от технологических и физических атак. Доработка корпоративной политики безопасности, поможет сотрудникам правильно реагировать на попытки заставить или убедить их предоставить доступ к корпоративным ресурсам или разгласить информацию, связанную с системой безопасности.

4.2. Угрозы, связанные с использованием методов социотехники

Атаки, основанные на методах социотехники, можно разделить на пять основных направлений.

- Сетевые атаки.
- Телефонные атаки.
- Поиск информации в мусоре.
- Персональные подходы.
- Обратная социотехника.

Кроме этого нужно также понимать, что рассчитывают получить злоумышленники. Злоумышленниками движут те же потребности, что и всеми людьми: деньги, социальный статус и самооценка. Иными словами, злоумышленники хотят получить чужие деньги или ресурсы, добиться признания в обществе или своей группе и возвысить себя в своих глазах. К сожалению, злоумышленники добиваются этих целей незаконными методами, воруя информацию или причиняя вред компью-

терным системам. Любые атаки могут нанести компании ущерб в виде финансовых убытков, траты ресурсов, утечки информации, снижения работоспособности компании и урона ее репутации. При разработке мер защиты от соответствующих угроз следует сначала оценить последствия атаки.

4.3. Сетевые угрозы

Злоумышленник, использующий методы социотехники, не пытается заразить корпоративную систему вредоносными программами в ходе прямой атаки. Вместо этого он обманным путем убеждает сотрудника компании предоставить ему нужную информацию, приводя обоснованные правдоподобные доводы. Полученную информацию злоумышленник может использовать для последующего проведения атак с помощью вредоносных программ, но к социотехнике это уже не относится. Сотрудники компании должны знать, как лучше всего определять и блокировать сетевые атаки, основанные на методах социотехники.

4.3.1. Угрозы, связанные с электронной почтой

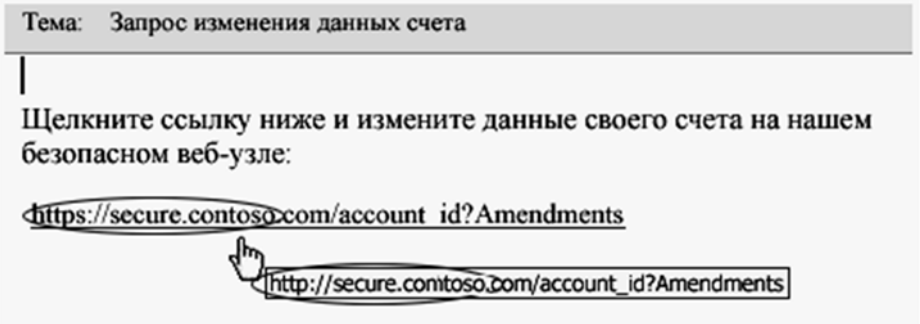
Многие сотрудники ежедневно получают через корпоративные и частные почтовые системы десятки и даже сотни электронных писем. Разумеется, при таком потоке корреспонденции невозможно уделить должное внимание каждому письму. Это значительно облегчает проведение атак, основанных на методах социотехники. Большинство пользователей систем электронной почты спокойно относятся к обработке таких сообщений, воспринимая эту работу как электронный аналог перекладывания бумаг из одной папки в другую. Когда злоумышленник присылает по почте простой запрос, его жертва часто выполняет то, о чем ее просят, не задумываясь о своих действиях.

Например, злоумышленник может отправить сотруднику компании письмо, в котором говорится об указании начальника прислать ему все расписания выходных дней для организации встречи, отправив копию ответа всем пользователям, включенным в прилагаемый список. Злоумышленник может легко включить в этот список внешний адрес и *подделать* имя отправителя, чтобы казалось, что письмо получено из внутреннего источника. Подделать данные особенно легко, если у злоумышленника есть доступ к корпоративной компьютерной системе, потому что в этом случае ему не могут помешать брандмауэры, защищающие периметр сети. Утечка информации о расписании выходных дней подразделения не кажется угрозой безопасности, но на самом

деле благодаря этому злоумышленник может узнать, кто из сотрудников компании и когда будет отсутствовать на своем рабочем месте. В это время злоумышленник сможет выдать себя за отсутствующего сотрудника с меньшим риском разоблачения.

В последнее десятилетие использование электронной почты в качестве средства проведения социотехнических атак приобрело очень высокую популярность. Получение личной или конфиденциальной информации у пользователей с помощью электронной почты называют *фишингом*. С этой целью злоумышленники могут использовать электронные письма, имитирующие письма реальных организаций, например банков и компаний-партнеров.

Например, на следующем рисунке показана на первый взгляд корректная ссылка на страницу управления учетной записью веб-узла компании Contoso.



Однако если приглядеться к ней внимательнее, можно заметить два несоответствия.

В тексте письма утверждается, что узел, на который указывает ссылка, защищен с помощью протокола https, тогда как по подсказке видно, что на самом деле при взаимодействии с этим узлом используется протокол http.

В тексте письма указано название компании Contoso, но на самом деле ссылка указывает на веб-узел компании Comtoso.

Используя фишинг, злоумышленник обычно действует наобум, просто запрашивая у пользователя информацию. Для придания правдоподобности таким письмам злоумышленники могут использовать в них корпоративные логотипы и шрифты и даже указывать реальные бесплатные телефоны службы поддержки. Информация у пользовате-

лей часто запрашивается под предлогом оказания помощи с обновлением систем или предоставления дополнительных услуг. Более продвинутой формой фишинга является *направленный фишинг (spear-phishing)* – атака, целью которой является конкретный сотрудник или группа сотрудников. Этот подход гораздо более сложен, поскольку в этом случае злоумышленник должен быть знаком с личными и важными корпоративными данными, чтобы его обман выглядел убедительно. Однако и вознаграждение злоумышленника при этом выше: добившись успеха, он получит более подробные и конкретные сведения.

Электронные письма могут содержать гиперссылки, склоняющие сотрудников к нарушению защиты корпоративной среды. Как показано на рис. 1, ссылки не всегда ведут на заявленные страницы. Есть целый ряд других вариантов фишинга с помощью электронной почты, в том числе применение изображений в качестве гиперссылок на вредоносные программы и включение текста в изображения ради обхода фильтров проверки гиперссылок.

Большинство мер по обеспечению безопасности направлены на предотвращение доступа неавторизованных пользователей к корпоративным ресурсам. Если, щелкнув присланную злоумышленником гиперссылку, пользователь загрузит в корпоративную сеть троянскую программу, вирус-червь или вирус, это позволит легко обойти многие виды защиты. Гиперссылка может также указывать на узел со всплывающими приложениями, запрашивающими данные или предлагающими помощь.

Для классификации атак и оценки риска, с которым сталкивается конкретная компания, можно использовать таблицу направлений, объектов и описаний атак и наносимого ими ущерба. Ниже показана именно такая таблица. С некоторыми угрозами связано сразу несколько факторов риска. Если это так, в приведенных ниже примерах главные факторы риска выделены жирным шрифтом.

Цели атаки	**Описание**	**Ущерб**
Кража корпоративной информации	Выдавая себя за внутреннего пользователя, злоумышленник пытается получить корпоративную информацию.	**Утечка конфиденциальной информации**
		Урон репутации компании
Кража финансовой информации	Используя методы фишинга (или направленного фишинга), злоумышленник запрашивает конфиденциальную корпоративную информацию, такую как учетные записи.	**Финансовые потери**
		Утечка конфиденциальной информации
		Урон репутации компании

Загрузка вредоносного ПО	Злоумышленник обманным путем убеждает пользователя щелкнуть гиперссылку или открыть вложение, что приводит к заражению корпоративной сети.	**Снижение работоспособности компании**
		Урон репутации компании
Загрузка ПО злоумышленника	Злоумышленник обманным путем убеждает пользователя щелкнуть гиперссылку или открыть вложение, в результате чего загружается программа злоумышленника, потребляющая ресурсы корпоративной сети.	**Трата ресурсов**
		Урон репутации компании
		Финансовые потери

Как и в случае с другими разновидностями мошенничества, самым эффективным способом защиты от атак злоумышленников, основанных на методах социотехники, является скептическое отношение к любым неожиданным входящим письмам. Для распространения этого подхода в организации в политику безопасности следует включить конкретные принципы использования электронной почты, охватывающие перечисленные ниже элементы.

- Вложения в документы.
- Гиперссылки в документах.
- Запросы личной или корпоративной информации, исходящие изнутри компании.
- Запросы личной или корпоративной информации, исходящие из-за пределов компании.

Кроме того, в описание этих принципов следует включить примеры атак, основанных на фишинге. Ознакомившись с примерами, пользователям будет проще выявлять другие попытки фишинга.

4.3.2. Всплывающие приложения и диалоговые окна

Едва ли можно рассчитывать, что сотрудники компании не будут использовать корпоративные средства доступа в Интернет в своих личных целях. Совершая покупки в интернет-магазинах, разыскивая интересующую их информацию и решая другие личные задачи, сотрудники (а значит и компания) могут стать жертвами злоумышленников, использующими методы социотехники. Даже если злоумышленников не интересует эта конкретная компания, они могут попытаться получить через сотрудников доступ к корпоративным ресурсам. Одной из самых популярных целей таких атак является встраивание в корпоративную среду почтового механизма, который будет использоваться для фишинга или проведения иных типов почтовых атак на системы других компаний или пользователей.

Чтобы убедить пользователя нажать кнопку в диалоговом окне, злоумышленники чаще всего отображают предупреждение о проблеме (например реалистичное сообщение об ошибке операционной системы или приложения) или предлагают дополнительные услуги, такие как возможность бесплатно загрузить программу, ускоряющую работу компьютера. Опытные пользователи обычно распознают в подобных ситуациях обман, однако людей, плохо знакомых с компьютерными технологиями и Интернетом, такие всплывающие приложения или диалоговые окна могут напугать или заинтересовать.

Защита пользователей от социотехнических атак, основанных на использовании всплывающих приложений, сводится преимущественно к информированию. Для устранения самих причин проблемы можно заблокировать в обозревателе Интернета всплывающие окна и автоматическую загрузку файлов, однако полностью исключить отображение всех всплывающих окон в обозревателе не получится. Поэтому лучше убедить пользователей не щелкать никакие ссылки во всплывающих окнах без ведома специалистов службы поддержки. Чтобы этот подход оправдал себя, сотрудники службы поддержки не должны осуждать пользователей за подключение к Интернету без служебной надобности. На это можно повлиять, приняв соответствующую корпоративную политику использования Интернета в личных целях.

Цели атаки	Описание	Ущерб
Кража личной информации сотрудников	Злоумышленник запрашивает у сотрудника компании личную информацию.	**Утечка конфиденциальной информации**
		Финансовые потери (для сотрудника)
Загрузка вредоносного ПО	Злоумышленник обманным путем убеждает пользователя щелкнуть гиперссылку или открыть вложение.	**Снижение работоспособности компании**
		Урон репутации компании
Загрузка ПО злоумышленника	Злоумышленник обманным путем убеждает пользователя щелкнуть гиперссылку или открыть вложение.	**Трата ресурсов**

4.3.3. Служба мгновенного обмена сообщениями

Мгновенный обмен сообщениями – сравнительно новый способ передачи данных, однако он уже приобрел широкую популярность среди корпоративных пользователей, и некоторые аналитики прогнозируют, что число пользователей таких систем достигнет в 2006 году 200 миллионов. Из-за быстроты и легкости использования этот способ коммуникации открывает широкие возможности для проведения со-

циотехнических атак: пользователи относятся к нему как к телефонной связи и не связывают с потенциальными программными угрозами. Двумя основными видами атак, основанных на использовании службы мгновенного обмена сообщениями, являются указание в теле сообщения ссылки на вредоносную программу и доставка самой программы. Конечно, мгновенный обмен сообщениями – это еще и один из способов запроса информации.

Мгновенный обмен сообщениями имеет несколько особенностей, которые облегчают проведение социотехнических атак. Одна из таких особенностей – его неформальный характер. В сочетании с возможностью присваивать себе любые имена этот фактор позволяет злоумышленнику гораздо легче выдавать себя за другого человека и значительно повышает его шансы на успешное проведение атаки, основанной на подделке данных.

Цели атаки	Описание	Ущерб
Получение конфиденциальной корпоративной информации	Подделывая мгновенные сообщения, злоумышленник выдает себя за сотрудника компании, чтобы запросить корпоративную информацию.	**Утечка конфиденциальной информации**
		Урон репутации компании
Загрузка вредоносного ПО	Злоумышленник обманным путем убеждает пользователя щелкнуть гиперссылку или открыть вложение, что приводит к заражению корпоративной сети.	**Снижение работоспособности компании**
		Урон репутации компании
Загрузка ПО злоумышленника	Злоумышленник обманным путем убеждает пользователя щелкнуть гиперссылку или открыть вложение, в результате чего происходит загрузка программы злоумышленника (например почтового механизма), потребляющей ресурсы корпоративной сети.	**Трата ресурсов**

Если компания намерена использовать возможности сокращения расходов и другие преимущества, обеспечиваемые мгновенным обменом сообщениями, необходимо предусмотреть в корпоративных политиках безопасности механизмы защиты от соответствующих угроз. Для получения надежного контроля над мгновенным обменом сообщениями в корпоративной среде выполните пять следующих требований.

Выберите одну платформу для мгновенного обмена сообщениями. Это облегчит работу службы поддержки и уменьшит вероятность того, что сотрудники будут пользоваться аналогичными службами других поставщиков. Если нужно надежнее ограничить имеющийся у пользователей выбор, можно заблокировать порты, используемые популярными службами мгновенного обмена сообщениями.

Определите параметры защиты, задаваемые при развертывании службы мгновенного обмена сообщениями. Клиентские модули систем мгновенного обмена сообщениями поддерживают различные параметры конфигурирования функций обеспечения безопасности и конфиденциальности, таких как поиск вирусов.

Определите принципы установления новых контактов. Порекомендуйте пользователям не принимать по умолчанию любые приглашения к общению.

Задайте стандарты выбора паролей. Потребуйте от сотрудников, чтобы их пароли к службе обмена сообщениями соответствовали стандартам выбора надежных паролей, которые приняты для паролей, служащих для входа в систему.

Составьте рекомендации по использованию службы мгновенного обмена сообщениями. Сформулируйте для пользователей службы мгновенного обмена сообщениями оптимальные принципы работы с ней, подкрепив рекомендации обоснованными доводами.

4.4. Угрозы, связанные с использованием телефона

Телефонная связь обеспечивает уникальные возможности для проведения социотехнических атак. Это очень привычное и в то же время обезличенное средство общения, поскольку жертва не может видеть злоумышленника. Коммуникационные функции, поддерживаемые большинством компьютерных систем, могут также сделать привлекательной мишенью корпоративные телефонные станции. Еще одним видом атак (весьма грубым) является кража ПИН-кодов кредитных и телефонных карт через телефонные будки. Чаще всего при этом крадется личная информация конкретных людей, но иногда злоумышленникам удается раздобыть таким способом и ПИН-коды корпоративных кредитных карт. Большинство людей довольно осторожны при вводе ПИН-кодов в банкоматы, но при пользовании общественными телефонами многие из них ведут себя более беспечно.

Средства голосовой связи через Интернет (VoIP) могут обеспечить компаниям значительную экономию, и их рынок быстро развивается. В настоящее время из-за сравнительно небольшого числа таких систем атаки на них не рассматриваются в качестве серьезной угрозы. Однако можно ожидать, что по мере роста популярности этой техноло-

гии подделка пакетов VoIP станет такой же распространенной, как и подделка писем и мгновенных сообщений.

4.4.1. Корпоративные телефонные станции

Злоумышленник, атакующий корпоративную телефонную станцию, может преследовать три основные цели.

- Запросить информацию (как правило, выдавая себя за легального пользователя), обеспечивающую доступ к самой телефонной системе или позволяющую получить удаленный доступ к компьютерным системам.
- Получить возможность совершать бесплатные телефонные звонки.
- Получить доступ к коммуникационной сети.

Все эти цели объединяет общий сценарий: злоумышленник звонит в компанию и пытается узнать телефонные номера, позволяющие получить доступ к самой корпоративной телефонной станции или опосредованный доступ через нее к телефонной сети общего пользования. Сами злоумышленники называют взлом телефонных систем словом *«фрикинг» (phreaking)*. Как правило, телефонные злоумышленники представляются инженерами по обслуживанию телефонных систем и запрашивают у сотрудника компании внешнюю линию или пароль якобы для анализа и устранения проблем с внутренней телефонной системой.

Запрос информации или доступа по телефону – сравнительно неопасный для злоумышленника вид атаки. Если жертва начинает что-то подозревать или отказывается выполнять запрос, злоумышленник может просто повесить трубку. Помните, однако, что в реальной жизни эти атаки бывают довольно изощренными. Злоумышленник не просит напрямую сказать ему идентификатор пользователя и пароль. Обычно он описывает правдоподобную ситуацию, прося о помощи или наоборот, предлагая ее, и лишь потом запрашивает личную или деловую информацию, как бы чуть не забыв об этом.

Цели атаки	Описание	Ущерб
Получение корпоративной информации	Выдавая себя за легального пользователя, злоумышленник пытается получить конфиденциальную информацию.	Утечка конфиденциальной информации
		Урон репутации компании
Получение информации о телефон-	Выдавая себя за инженера по обслуживанию телефонных систем, злоумышленник пытается по-	Трата ресурсов
		Финансовые

ной системе	лучить доступ к корпоративной телефонной станции с целью совершения внешних телефонных звонков.	потери
Использование корпоративной телефонной станции для доступа к компьютерным системам	Используя корпоративную телефонную станцию, злоумышленник получает доступ к компьютерным системам для кражи или изменения информации, заражения систем вредоносным ПО или использования ресурсов в своих целях.	

Большинство пользователей ничего не знают о внутренней телефонной системе компании, исключая, конечно, сам телефон. Это и есть самый важный рубеж защиты, который можно определить в политике безопасности и который в своих целях часто пытаются использовать злоумышленники. Чаще всего жертвами при этом являются сотрудники приемной или сотрудники, работающие с коммутатором. В политике нужно указать, что только специалисты службы поддержки имеют право оказывать помощь по телефону. Благодаря этому все обращения за технической помощью будут обрабатывать только авторизованные сотрудники. Этот подход позволяет также организовать быстрое и эффективное перенаправление таких запросов квалифицированным специалистам.

4.4.2. Служба поддержки

Служба поддержки – один из главных механизмов защиты от обычных злоумышленников и в то же время частая мишень злоумышленников, использующих методы социотехники. Многие сотрудники служб поддержки знают и помнят об угрозах, но сама суть их работы предполагает, что они должны оказывать пользователям помощь и давать рекомендации. Иногда энтузиазм специалистов служб технической поддержки превосходит их готовность следовать процедурам обеспечения безопасности, и тогда возникает проблема. Если они решат строго соблюдать стандарты безопасности, запрашивая у пользователей подтверждения их подлинности, они могут показаться бесполезными или даже произвести неприятное впечатление. Сотрудники производственных отделений или менеджеры по продажам и маркетингу, считающие, что ИТ-отделение не удовлетворило их требования, склонны жаловаться; руководителям высшего звена также часто не нравится дотошность службы поддержки, если они сталкиваются с ней сами.

Цели атаки	Описание	Ущерб
Получение информации	Выдавая себя за легального пользователя, злоумышленник пытается получить деловую информацию.	**Утечка конфиденциальной информации**

Получение доступа	Выдавая себя за легального пользователя, злоумышленник пытается получить доступ к корпоративным системам.	**Утечка конфиденциальной информации; Урон репутации компании; Снижение работоспособности компании; Трата ресурсов;** Финансовые потери

Службе поддержки следует найти баланс между безопасностью и эффективностью работы и отразить достигнутый компромисс в политиках и процедурах безопасности. Едва ли, например, кто-нибудь из сотрудников будет протестовать, если при обращении в службу поддержки его попросят назвать свой номер, отделение и фамилию начальника. Конечно, это недостаточно надежная защита, так как злоумышленник может украсть эту информацию, но для начала и этот подход неплох. На самом деле единственным методом идентификации с точностью 99,99 % является тест ДНК, использовать который явно не представляется возможным.

Защитить службу поддержки от атак со стороны внутреннего сотрудника или подрядчика сложнее. Злоумышленники из их числа хорошо разбираются во внутренних процедурах компании и будут действовать наверняка, собрав перед обращением в службу поддержки всю необходимую информацию. Процедуры обеспечения безопасности должны выполнять в таких ситуациях две следующих функции.

Служба поддержки должна гарантировать, что все действия пользователей, обращающихся за помощью, регистрируются. Если, обратившись в службу поддержки, злоумышленник возможность несанкционированного доступа к данным и ресурсам, регистрация его действий позволит быстро заблокировать атаку и ограничить причиненный ущерб. Кроме того, при каждом обращении в службу поддержки целесообразно генерировать автоматически или создавать вручную почтовое сообщение с описанием проблемы или запроса и отправлять его заинтересованным лицам. Это поможет сотруднику, у которого украли учетные данные, понять, что произошло, и обратиться в службу поддержки.

Служба поддержки должна утвердить структурированную процедуру обработки разных типов запросов. Например, если запрашивать изменения прав доступа для сотрудника должен будет по электронной почте его начальник, это исключит несанкционированные или неформальные изменения уровней безопасности.

Если пользователи будут знать эти правила, а руководители поддержат их реализацию, злоумышленникам будет гораздо труднее проводить атаки и оставаться безнаказанными. Полный аудиторский контроль – самое эффективное средство обнаружения и предотвращения нарушений законов и корпоративных норм.

4.5. Угрозы, связанные с утилизацией мусора

Несанкционированный анализ мусора – или, как это еще называют, *«ныряние в мусорные контейнеры»* – часто позволяет злоумышленникам получить ценную информацию. Бумажные отходы компании могут содержать сведения, которые злоумышленник может использовать напрямую (например номера учетных записей и идентификаторы пользователей) или которые облегчают ему проведение дальнейших атак (списки телефонов, схемы структуры организации и т. д.). Для злоумышленника, использующего социотехнику, сведения второго типа особенно ценны, потому что они помогают ему проводить атаки, не вызывая подозрения. Например, зная имена и фамилии людей, работающих в определенном подразделении компании, злоумышленник имеет гораздо больше шансов при поиске подхода к ее сотрудникам, большинству из которых будет легко поверить, что человек, так много знающий о компании, является их коллегой.

Электронные средства хранения информации бывают для злоумышленников еще более полезными. Если в компании не действуют правила сбора отходов, предусматривающие утилизацию списанных носителей данных, на выброшенных жестких дисках, компакт-дисках и дисках DVD можно найти самые разнообразные сведения. Современные электронные носители данных надежны и долговечны, поэтому службы, отвечающие за защиту ИТ-систем, должны обеспечить соблюдение политик, предусматривающих уничтожение этих носителей или стирание хранящихся на них данных.

Цели атаки	Описание	Ущерб
Бумажный мусор в мусорных корзинах, расположенных вне организации	Изучая документы, извлеченные из внешних мусорных контейнеров, злоумышленник узнает важную корпоративную информацию.	**Утечка конфиденциальной информации**
		Урон репутации компании
Бумажный мусор в мусорных корзинах, расположенных внутри организации	Обходя принятые в организации принципы управления внешним мусором, злоумышленник ворует документы из мусорных корзин, расположенных в самой организации.	**Утечка конфиденциальной информации**
		Урон репутации компании
Выброшенные	Злоумышленник ворует данные и приложения,	**Утечка конфиден-**

электронные носители	хранящиеся на выброшенных электронных носителях, и сами носители.	**циальной информации**

Сотрудники компании должны понимать все последствия, к которым может привести выбрасывание бумажных документов или электронных носителей информации в мусорную корзину. Как только мусор покидает территорию компании, ее права могут больше на него не распространяться. Само по себе «ныряние в мусоре» не всегда является чем-то незаконным, поэтому сотрудники компании должны знать, что нужно делать с мусором. Бумажный мусор всегда следует измельчать в бумагорезательных машинах, а электронный – уничтожать или стирать записанные на нем данные. Если какие-либо документы (например телефонный справочник) из-за размеров или жесткости невозможно измельчить в бумагорезательной машине либо у пользователя нет технической возможности это сделать, нужно определить специальную процедуру избавления от них. Мусорные контейнеры следует размещать в защищенной области, недоступной посторонним лицам.

При разработке политики утилизации мусора важно убедиться в том, что соблюдены все местные санитарные нормы и нормы безопасности. По мере возможности следует выбирать экологически чистые способы утилизации мусора.

Кроме внешнего мусора – бумажных или электронных отходов, доступных посторонним лицам, – есть еще и внутренний, который тоже нужно контролировать. При определении политик безопасности это часто упускают из виду, предполагая, что любому, кто имеет доступ на объекты компании, можно доверять. Ясно, что это не всегда так. Одной из самых эффективных мер по управлению бумажным мусором является классификация данных. Для этого следует определить разные категории бумажных документов и способы их утилизации. Ниже перечислены примеры таких категорий.

4.6. Персональные подходы

Самый простой и дешевый для злоумышленника способ получить нужную ему информацию – непосредственно запросить ее. Каким бы грубым и банальным этот способ ни казался, он неизменно остается главным в арсенале злоумышленников, использующих методы социотехники. Для получения информации с помощью этого способа злоумышленники используют четыре стратегии.

Запугивание. Злоумышленники, выбравшие эту стратегию, часто заставляют жертву выполнить запрос, выдавая себя за лиц, облеченных властью.

Убеждение. Самые популярные формы убеждения – лесть и ссылки на известных людей.

Вызов доверия. Этот подход обычно требует достаточно длительного времени и связан с формированием доверительных отношений с коллегой или начальником ради получения у него в конечном итоге нужной информации.

Помощь. Злоумышленник, выбравший этот подход, предлагает сотруднику компании помощь, для оказания которой якобы нужна личная информация сотрудника. Получив эту информацию, злоумышленник крадет идентификационные данные жертвы.

В контексте социотехники интересен тот факт, что большинство людей, признавая, что сами иногда лгут, исходят из того, что другие всегда говорят им правду. Безоговорочное доверие – одна из целей злоумышленника, использующего методы социотехники.

Защитить пользователей от атак, основанных на описанных персональных подходах, очень сложно. Некоторые пользователи в силу своего характера имеют больше шансов стать жертвами атак, основанных на каком-либо из четырех этих подходов. Защититься от атак, основанных на запугивании, можно, способствуя формированию корпоративной культуры, исключающей страх. Если сотрудники компании всегда ведут себя вежливо и учтиво, запугивание не позволит злоумышленнику добиться желаемого, потому что подвергшийся атаке сотрудник скорее всего сообщит об этом начальству. Благожелательное отношение к сотрудникам со стороны руководства и надзор за процедурой решения проблем и принятия решений – худшее, с чем может столкнуться злоумышленник, использующий методы социотехники. Ему нужно, чтобы жертвы атак принимали решения быстро. Если в компании принято докладывать о проблемах руководителям, злоумышленник этого не добьется.

Убеждение всегда было важным способом достижения личных целей. Полностью исключить вероятность успешного проведения атак, основанных на убеждении, нельзя, но сотрудникам можно дать четкие указания по поводу того, что им следует делать, а что не следует. Пытаясь получить конфиденциальную информацию методом убеждения,

злоумышленники всегда представляют тот или иной сценарий, предполагающий, что пользователь сообщит ее добровольно. Регулярное проведение информационных кампаний и определение базовых принципов использования паролей и других средств обеспечения безопасности – лучшая защита от подобных атак.

Чтобы войти в доверие к сотрудникам компании, злоумышленнику нужно время. Злоумышленник должен регулярно общаться с сотрудниками, что значительно легче, если он работает вместе с ними. В большинстве компаний среднего размера основным источником таких угроз являются работники, регулярно оказывающие компании какие-либо услуги или работающие по контракту. Поэтому отдел кадров должен уделять подбору сотрудников, работающих по контракту, не меньше внимания, чем найму постоянных сотрудников. Основную часть этой работы можно делегировать кадровому агентству. Для гарантии того, что агентство справится с этой задачей, можно потребовать, чтобы им были соблюдены принятые в компании политики подбора постоянных сотрудников. Если есть подозрение, что на постоянную работу в компанию устроился злоумышленник, использующий методы социотехники, лучшими способами защиты от него являются информирование сотрудников и соблюдение ими политики информационной безопасности.

Наконец, вероятность успешного проведения атак, основанных на злоупотреблении взаимопомощью, можно свести к минимуму, обеспечив высокую эффективность работы службы поддержки. Зачастую сотрудники обращаются за помощью к коллегам из-за неудовлетворенности услугами имеющейся службы поддержки. Чтобы гарантировать, что в случае проблем сотрудники будут обращаться в службу поддержки, а не к коллегам или, хуже того, к внешним специалистам, необходимо выполнить два условия.

Укажите в политике безопасности, что при возникновении проблем пользователи могут запрашивать помощь только у специалистов службы поддержки и ни у кого больше.

Убедитесь в том, что для службы поддержки определена процедура реагирования на проблемы, отраженная в принятом для отделения компании соглашении об уровне обслуживания. Регулярно проводите аудит эффективности работы службы поддержки, проверяя, чтобы пользователи получали всю необходимую помощь.

Служба поддержки – важный механизм защиты от социотехнических атак, который не стоит недооценивать.

4.6.1. Виртуальные методы

Для проведения атаки, основанной на социотехнике, злоумышленнику нужно установить контакт с жертвой. Как правило, для этого он использует электронные способы взаимодействия, такие как электронная почта или всплывающие окна. Из-за увеличения числа нежелательных писем, получаемых большинством пользователей, эффективность этого метода атак снизилась, так как пользователи стали более скептически относиться к письмам, присланным по цепочке, и предложениям принять участие в «законных» прибыльных финансовых операциях. И все же, несмотря на сравнительную неэффективность этого метода, объем нежелательной корреспонденции и многочисленные попытки проведения атак с помощью троянских почтовых программ говорят о том, что некоторые злоумышленники не спешат отказываться от старых методик. В большинстве случаев эти атаки направлены на конкретных людей и проводятся с целью получения идентификационных данных жертвы. Однако из-за частого использования корпоративных компьютеров, средств доступа в Интернет и других бизнес-систем в личных целях такие атаки представляют угрозу и для компаний.

Телефонные технологии позволяют злоумышленникам устанавливать более личные, но менее массовые контакты с жертвами. Из-за низкой вероятности ареста некоторые злоумышленники рассматривают телефон как одно из главных средств социотехнических атак, но область применения этого метода во многом ограничена атаками на корпоративную телефонную станцию и службу поддержки. Это объясняется тем, что большинство пользователей с подозрением относятся к звонкам с запросами информации, исходящим от незнакомцев.

4.6.2. Физические методы

Менее популярным, но более эффективным для злоумышленника способом подготовки к проведению атаки является установление непосредственного личного контакта с жертвой. Только самые недоверчивые сотрудники способны усомниться в искренности человека, лично просящего помощи в решении компьютерных проблем или предлагающего такую помощь. Хотя такие способы связаны для злоумышленника с гораздо большим риском, они обеспечивают ему ряд преимуществ. В случае успеха он получает свободный доступ к корпо-

ративным системам изнутри компании, обойдя все технические средства защиты периметра.

Другой серьезной угрозой для компаний является распространение мобильных технологий, позволяющих пользователям подключаться к корпоративным сетям дома и в пути. Это делает возможными самые разные атаки: от совсем простых, основанных на наблюдении за тем, как пользователь вводит в ноутбук идентификатор и пароль, до довольно сложных, при которых злоумышленник, выдавая себя за услужливого сотрудника службы поддержки, приносит и устанавливает обновление для устройства чтения карт или маршрутизатора, попутно попросив у пользователя идентификатор и пароль для доступа к корпоративной сети (а иногда еще и чашечку кофе). Идущий до конца злоумышленник может даже попросить и получить от пользователя электронную подпись, используемую для проверки его полномочий. В качестве другого примера атак этого рода можно привести использование оплаченных компанией ресурсов для доступа в Интернет через незащищенную беспроводную сеть.

Хотя в большинстве крупных компаний имеется развитая инфраструктура ограничения доступа на корпоративные объекты, в компаниях малого и среднего размера этим часто пренебрегают. Это обеспечивает возможность проведения очень простых социотехнических атак, основанных на *несанкционированном проникновении в офисное здание* вместе с сотрудником компании, имеющим пропуск. Злоумышленник придерживает дверь перед законным пользователем, заводит с ним разговор на какую-нибудь банальную тему и проходит вместе с ним через пропускной пункт, не вызывая подозрения у контролеров. Для атак на крупные компании, сотрудники которых могут пройти в здание только через турникеты, считывающие данные с электронных карт, и малые организации, где все друг друга знают, этот подход не годится. Однако для атак на компании, насчитывающие около тысячи сотрудников, далеко не всегда знакомых друг с другом, он подходит как нельзя лучше. Если злоумышленнику ранее удалось получить корпоративную информацию, например названия подразделений, фамилии сотрудников или данные из внутренних служебных записок, ему будет проще завязать разговор.

Обеспечение безопасности систем сотрудников, работающих дома, обычно ограничивается техническими средствами. Политика безопасности должна требовать, чтобы домашние системы этих сотрудников были защищены брандмауэрами, блокирующими попытки зло-

умышленников получить доступ к сети извне. Других требований к обеспечению безопасности и даже резервному копированию данных, выполняемому сотрудниками дома, в большинстве компаний среднего размера нет.

Цели атаки	Описание	Ущерб
Кража учетных данных мобильного пользователя	Злоумышленник подсматривает, как легальный пользователь вводит в систему учетные данные или другие сведения. Это может предшествовать краже мобильного компьютера.	Утечка конфиденциальной информации
Кража учетных данных сотрудника, работающего дома	Злоумышленник представляется специалистом службы поддержки, чтобы получить доступ к сети пользователя, работающего дома, и запрашивает у пользователя идентификатор и пароль якобы для тестирования обновленной конфигурации системы.	Утечка конфиденциальной информации
Вход в корпоративную сеть через сеть сотрудника, работающего дома.	Выдавая себя за представителя службы поддержки, злоумышленник получает доступ к сети сотрудника, работающего дома, и использует ее для подключения к корпоративной сети. В случае успеха злоумышленник получает свободный доступ к сети и ресурсам компании.	Утечка конфиденциальной информации Урон репутации компании Снижение работоспособности компании Трата ресурсов Финансовые потери
Текущий доступ к сети сотрудника, работающего дома	Злоумышленник или локальный пользователь получает доступ в Интернет по широкополосному соединению, используя для этого незащищенную домашнюю сеть другого пользователя.	Трата ресурсов
Доступ в офисное здание компании без сопровождения	Злоумышленник проникает в офисное здание компании вслед за авторизованным сотрудником.	Утечка конфиденциальной информации Урон репутации компании Снижение работспособности компании Финансовые потери Трата ресурсов
Доступ в офис сотрудника компании	Злоумышленник получает доступ в офис сотрудника компании, где пытается воспользоваться компьютерным оборудованием или найти интересующие его сведения в бумажных документах.	Утечка конфиденциальной информации Трата ресурсов Финансовые потери

Защита от этих угроз во многом сводится к реализации оптимальных методик работы на основе эффективной корпоративной политики безопасности, которая должна охватывать три области:

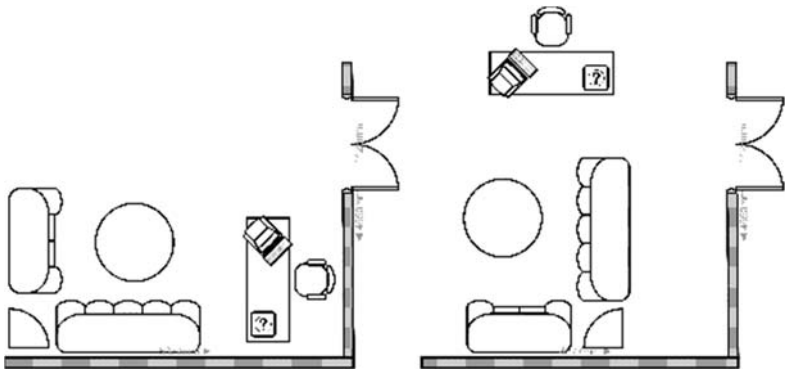
- здание компании;
- домашние системы;
- мобильные системы, используемые для работы.

Возможность проникновения в здание или на объект компании без прохождения авторизации должна быть исключена. Взаимодействуя с работниками компании, подрядчиками и посетителями, служащие приемной должны быть вежливыми, но непреклонными. Включив в корпоративную политику безопасности несколько простых принципов, вероятность проведения социотехнических атак в здании можно свести практически к нулю. Эти принципы могут определять перечисленные ниже требования.

- Использование идентификационных карт с фотографиями, демонстрируемых каждый раз при входе в здание компании и выходе из него.
- Ведение книги учета посетителей, в которой посетитель и сотрудник, к которому он явился, должны поставить свои подписи при прибытии посетителя и его уходе.
- Применение датированных пропусков посетителей, прикрепляемых на одежду в видном месте и возвращаемых служащему приемной при выходе из здания.
- Ведение книги учета подрядчиков, в которой подрядчик и сотрудник компании, утвердивший его рабочее задание, должны поставить свои подписи при прибытии подрядчика и его уходе.
- Применение датированных пропусков подрядчиков, прикрепляемых на одежду в видном месте и возвращаемых служащему приемной при выходе из здания.

Чтобы гарантировать, что все посетители будут представляться служащему приемной, нужно организовать барьеры, не позволяющие проникнуть в здание компании без его ведома и без выполнения регистрационных процедур. Использовать для этого турникеты или что-либо подобное необязательно.

Например, для организации потока посетителей через приемную можно использовать диван.



План, показанный слева, облегчает *несанкционированное проникновение на территорию компании*, позволяя злоумышленнику скрыться за подлинным сотрудником компании. Если же доступ в компанию организован по изображенной справа схеме, никакой посетитель не сможет пройти мимо стола служащего приемной незамеченным. Кроме того, в этом случае компьютер не ограничивает имеющийся у служащего приемной обзор. Проход на территорию компании нужно сделать достаточно широким, чтобы посетители, в том числе люди в инвалидных колясках, не испытывали никаких неудобств. Встречая и регистрируя каждого посетителя, служащие приемной должны вести себя профессионально и последовательно. Каждый вход в здание компании нужно привести в соответствие этим стандартам, запретив сотрудникам использование других входов и выходов – любые черные ходы должны отсутствовать.

При установке каких-либо барьеров или пропускных систем необходимо убедиться, что соблюдены все санитарные нормы, правила техники безопасности и права инвалидов.

Что касается домашних систем, то реализовать в них средства авторизации всех гостей и коммивояжеров невозможно. Однако на самом деле большинство людей при визите посетителей к ним домой ведут себя гораздо более осмотрительно, чем в такой же ситуации на работе. Таким образом, важнее гарантировать, что злоумышленник не сможет получить доступ к корпоративным ресурсам. Протокол оказания ИТ-услуг вне территории компании должен включать следующие правила.

• Все услуги технической поддержки, в том числе восстановление работоспособности систем и обновление их конфигурации на местах, должны планироваться и утверждаться службой поддержки.

• Подрядчики и штатные сотрудники, устанавливающие или обслуживающие системы на местах, должны иметь удостоверения, желательно с фотографией.

• Пользователи должны сообщать в службу поддержки время прибытия и отъезда ее представителя.

• На каждое задание должен выдаваться наряд на работу, подписываемый пользователем.

• Пользователи никогда не должны сообщать специалисту службы поддержки свои учетные данные или регистрироваться в системе ради того, чтобы он мог получить доступ к тем или иным ресурсам.

Последний пункт заслуживает особого внимания. Предоставлять специалистам по поддержке систем информацию, достаточную для выполнения работы, должен отдел обслуживания ИТ-систем. Если у инженера, прибывшего к пользователю, нет нужных прав доступа, он должен обратиться в службу поддержки. Это требование очень важно, потому что скромная должность сотрудника компании, занимающейся обслуживанием компьютеров, как нельзя лучше подходит для проведения атак. Она позволяет злоумышленнику демонстрировать свою принадлежность к официальным техническим службам и в то же время предлагать помощь.

Мобильные сотрудники часто используют свои компьютеры в поездах, аэропортах, ресторанах и других людных местах. Ясно, что исключить возможность наблюдения за сотрудником в таких условиях нельзя, но в корпоративную политику безопасности все равно нужно включить рекомендации по уменьшению риска кражи личной и корпоративной информации таким способом. Если сотрудники компании используют карманные ПК, в политике безопасности следует определить принципы управления защитой этих систем и синхронизации данных.

4.7. Обратная социотехника

Об *обратной социотехнике* говорят тогда, когда жертва или жертвы сами предлагают злоумышленнику нужную ему информацию. Это может показаться маловероятным, но на самом деле лица, обладающие авторитетом в технической или социальной сфере, часто получают идентификаторы и пароли пользователей и другую важную личную информацию просто потому, что никто не сомневается в их порядочности. Например, сотрудники службы поддержки никогда не спрашивают у пользователей идентификатор или пароль; им не нужна эта информация для решения проблем. Однако многие пользователи ради

скорейшего устранения проблем добровольно сообщают эти конфиденциальные сведения. Злоумышленнику даже не нужно спрашивать об этом. Тем не менее, социотехнические атаки в большинстве случаев инициируются злоумышленником.

Обычно злоумышленник, использующий методы социотехники, создает проблемную ситуацию, предлагает решение и оказывает помощь, когда его об этом просят. Рассмотрим следующий простой сценарий.

Злоумышленник, работающий вместе с жертвой, изменяет на ее компьютере имя файла или перемещает его в другой каталог. Когда жертва замечает пропажу файла, злоумышленник заявляет, что может все исправить. Желая быстрее завершить работу или избежать наказания за утрату информации, жертва соглашается на это предложение. Злоумышленник заявляет, что решить проблему можно, только войдя в систему с учетными данными жертвы. Он даже может сказать, что корпоративная политика запрещает это. Теперь уже жертва просит злоумышленника войти в систему под ее именем, чтобы попытаться восстановить файл. Злоумышленник неохотно соглашается и восстанавливает файл, а по ходу дела крадет идентификатор и пароль жертвы. Успешно осуществив атаку, он даже улучшил свою репутацию, и вполне возможно, что после этого к нему будут обращаться за помощью и другие коллеги. Этот подход не пересекается с обычными процедурами оказания услуг поддержки и осложняет поимку злоумышленника.

Не все атаки, основанные на обратной социотехнике, требуют, чтобы злоумышленник был знаком с жертвой или хотя бы встретился с ней. Добиться своего злоумышленник может, имитируя проблемы с помощью диалоговых окон. Как правило, при такой атаке на экране компьютера жертвы отображается окно с уведомлением о проблеме или необходимости обновления конфигурации системы. В этом же окне приводится ссылка на соответствующее обновление или исправление. После загрузки и установки файла сфабрикованная проблема исчезает, и пользователь продолжает работу, не подозревая о том, что он установил вредоносную программу.

Атаки, основанные на методах обратной социотехники, и возможный ущерб от них

Цели атаки	**Описание**	**Ущерб**
Кража учет-	Злоумышленник получает идентификатор	Утечка конфиденциальной

ных данных	и пароль авторизованного пользователя.	информации Урон репутации компании Снижение работоспособности компании Финансовые потери Трата ресурсов
Кража информации	Используя идентификатор и пароль авторизованного пользователя, злоумышленник получает доступ к файлам компании.	**Утечка конфиденциальной информации** **Финансовые потери** **Трата ресурсов** Урон репутации компании Снижение работоспособности компании
Загрузка вредоносного ПО	Злоумышленник обманным путем убеждает пользователя щелкнуть гиперссылку или открыть вложение, что приводит к заражению корпоративной сети.	**Снижение работоспособности компании** Урон репутации компании
Загрузка ПО злоумышленника	Злоумышленник обманным путем убеждает пользователя щелкнуть гиперссылку или открыть вложение, в результате чего происходит загрузка программы злоумышленника (например почтового механизма), потребляющей ресурсы корпоративной сети.	**Трата ресурсов** **Урон репутации компании** Финансовые потери

Защититься от атак, основанных на обратной социотехнике, наверное, сложнее всего. У жертвы нет оснований подозревать злоумышленника в чем-либо, так как при таких атаках создается впечатление, что ситуация находится под ее контролем. Главным способом защиты от атак, основанных на обратной социотехнике, является включение в политику безопасности принципа, требующего, чтобы все проблемы разрешались только через службу поддержки. Если специалисты службы поддержки будут компетентны, вежливы и терпимы, у сотрудников компании не будет повода обращаться за помощью к кому-либо другому.

4.8. Реализация мер защиты от атак, основанных на методах социотехники

После того, как политика безопасности задокументирована и утверждена, нужно проинформировать о ней сотрудников и разъяснить им важность ее соблюдения. Технические средства защиты можно внедрить и без участия сотрудников, но при реализации мер защиты от социотехнических атак без поддержки сотрудников обойтись не удастся. Чтобы облегчить реализацию этих мер, нужно разработать для службы поддержки протоколы реагирования на инциденты.

Информирование

Ничто так не облегчает реализацию социотехнических элементов политики безопасности, как удачная кампания по информированию сотрудников. Конечно, такую кампанию тоже можно рассматривать как разновидность социотехники. В ходе ее реализации нужно позаботиться о том, чтобы сотрудники ознакомились с политикой безопасности, поняли, зачем она нужна, и запомнили, что нужно делать, заподозрив атаку. Ключевой элемент социотехнических атак – доверие. Чтобы злоумышленник добился своего, жертва должна ему доверять. Для защиты от таких атак нужно привить сотрудникам разумное скептическое отношение ко всему неожиданному и внушить им доверие к корпоративной службе технической поддержки.

Элементы кампании по информированию сотрудников зависят от того, как в организации принято сообщать информацию. Для информирования о политиках безопасности можно выбрать структурированные обучающие курсы, неформальные встречи, плакаты и другие средства. Чем убедительнее будут представлены политики, тем эффективнее пройдет их реализация. Начать кампанию по информированию о проблемах безопасности можно с крупного мероприятия, но не менее важно регулярно напоминать о них руководителям и сотрудникам. Обеспечение безопасности – задача всей компании, и к ее решению следует привлечь по возможности всех сотрудников. Постарайтесь учесть мнения представителей всех подразделений и пользователей разных категорий, особенно тех, которые работают вне офисов.

Управление инцидентами

Получив информацию о социотехнической атаке, сотрудники службы поддержки должны знать, как действовать в сложившейся ситуации. В политике безопасности должны быть определены протоколы реагирования, но один из принципов управления инцидентами заключается в том, что в ответ на атаку проводится дополнительный аудит безопасности. Направления атак изменяются, поэтому обеспечение безопасности – это путь, не имеющий конца.

Каждый инцидент предоставляет новую информацию для текущего аудита безопасности в соответствии с моделью реагирования на инциденты:

1. Разрешение и анализ проблем.
2. Оценка рисков.
3. Создание или изменение политик безопасности.
4. Доведение сведений об изменениях в политиках до персонала.

При регистрации инцидента руководящий комитет по обеспечению безопасности должен выяснить, представляет ли он для компании новую или измененную угрозу, и, опираясь на сделанные выводы, создать или обновить политики и процедуры. Все поправки, вносимые в политики безопасности, должны соответствовать корпоративным стандартам управления изменениями.

Для управления инцидентами служба поддержки должна использовать утвержденный протокол, регистрируя в нем следующую информацию:

- Жертва атаки
- Подразделение жертвы
- Дата
- Направление атаки
- Описание атаки
- Результат атаки
- Последствия атаки
- Рекомендации

Регистрация инцидентов позволяет определить шаблоны атак и улучшить защиту от будущих атак. Образец бланка отчета об инциденте можно найти в приложении 1.

Рекомендации по работе

При выполнении аудита безопасности не следует чересчур увлекаться защитой компании от всевозможных потенциальных угроз. Политика безопасности должна отражать главную цель любой коммерческой компании – получение прибыли. Если предполагаемые меры защиты компании отрицательно скажутся на ее прибыльности или конкурентоспособности, возможно, риск следует оценить заново. Необходимо найти баланс между обеспечением безопасности и удобством и эффективностью работы.

С другой стороны, важно понимать, что репутация компании, уделяющей большое внимание безопасности, также обеспечивает коммерческие преимущества. Это не только отпугивает злоумышленников, но и вызывает доверие к компании у ее клиентов и партнеров.

Социотехника и комплексная многоуровневая модель обеспечения безопасности

В комплексной многоуровневой модели обеспечения безопасности решения для защиты компьютерных систем классифицируются в соответствии с направлениями атак – слабостями, которые злоумышленники могут использовать для реализации угроз. Ниже перечислены некоторые направления атак.

• **Политики, процедуры и информированность сотрудников.** Выраженные в письменной форме правила, регламентирующие управление всеми аспектами обеспечения безопасности, и образовательные программы, помогающие сотрудникам понять эти правила и соблюдать их.

• **Физическая безопасность.** Барьеры, ограничивающие доступ в здания компании и к корпоративным ресурсам. Не забывайте про ресурсы компании; например, мусорные контейнеры, расположенные вне территории компании, физически не защищены.

• **Данные.** Деловая информация: учетные записи, почтовая корреспонденция и т. д. При анализе угроз, связанных с использованием социотехники, и планировании мер по защите данных нужно определить принципы обращения с бумажными и электронными носителями данных.

• **Приложения.** Программы, запускаемые пользователями. Для защиты среды необходимо учесть, как злоумышленники, применяющие методы социотехники, могут использовать в своих целях почтовые программы, службы мгновенной передачи сообщений и другие приложения.

• **Компьютеры.** Серверы и клиентские системы, используемые в организации. Защитите пользователей от прямых атак на их компьютеры, определив строгие принципы, указывающие, какие программы можно использовать на корпоративных компьютерах и как следует управлять такими средствами обеспечения безопасности, как идентификаторы пользователей и пароли.

• **Внутренняя сеть.** Сеть, посредством которой взаимодействуют корпоративные системы. Она может быть локальной, глобальной или беспроводной. В последние годы из-за роста популярности методов удаленной работы границы внутренних сетей стали во многом условными. Сотрудникам компании нужно разъяснить, что они должны делать для организации безопасной работы в любой сетевой среде.

• **Периметр сети.** Граница между внутренними сетями компании и внешними, такими как Интернет или сети партнерских организаций, возможно, входящие в экстрасеть. Используя методы социотехники,

злоумышленники часто пытаются проникнуть через периметр сети, чтобы получить возможность проведения атак на данные, приложения и компьютеры во внутренней сети.

При разработке средств защиты комплексная модель обеспечения безопасности поможет лучше представить области бизнеса, которые подвергаются угрозам. Она охватывает не только социотехнические угрозы, но средства защиты от угроз этого рода должны быть реализованы на каждом уровне модели.

Самыми общими средствами защиты в этой модели являются политики безопасности, процедуры и информирование персонала. Они ориентированы на сотрудников организации и определяют, кто, что, когда и почему должен делать. Остальные уровни позволяют настроить средства обеспечения безопасности в соответствии со специфическими требованиями, но главным фактором защиты ИТ-среды все равно является структурированный набор правил, известных всем сотрудникам организации.

Далее в данном разделе представлены шаблоны таблиц, служащих для учета уязвимостей для атак, основанных на социотехнике, и определения требований политики обеспечения безопасности.

Уязвимости корпоративной среды, допускающие проведение атак, основанных на методах социотехники

Направление атаки	Нынешнее положение дел	Комментарии
Сетевые атаки		
Электронная почта		
Интернет		
Всплывающие приложения		
Служба мгновенного обмена сообщениями		
Телефонные атаки		
Корпоративная телефонная станция		
Служба поддержки		
Поиск информации в мусоре		
Внутренний мусор		
Внешний мусор		
Персональные подходы		
Физическая безопасность		
Безопасность офисов		
Другие направления атак и уязвимости, специфические для компании		

Форма для руководящего комитета, служащая для определения требований к обеспечению безопасности и оценки факторов риска

Направление атаки	Возможные требования политик	Тип риска: утечка конфиденциальной информации, урон репутации компании, снижение работоспособности компании, трата ресурсов, финансовые потери	Уровень риска: 5 = высокий 1 = низкий	Действие
Сетевые атаки				
Телефонные атаки				
Поиск информации в мусоре				
Персональные подходы				
Другие направления атак и уязвимости, специфические для компании				

Требования к процедурам и документации, определяемые руководящим комитетом

Требования политик	Требования к процедурам и документации	Дата выполнения действия

Реализация политики безопасности: контрольный список

Действие	Описание	Дата выполнения действия
Разработка политик защиты от сетевых угроз		
Разработка политик обеспечения физической безопасности		
Разработка политик защиты от угроз, связанных с использованием телефонных технологий		
Разработка политик безопасности, регламентирующих утилизацию мусора		
Разработка политик, регламентирующих безопасную работу службы поддержки		
Разработка модели реагирования на инциденты		
Разработка кампании по информированию сотрудников об угрозах		
...		

Отчет об инциденте

Представитель службы поддержки	
Жертва атаки	
Подразделение жертвы	
Дата	
Направление атаки	

Описание атаки	
Результат атаки	
Последствия атаки	
Рекомендации	

4.9. Проектирование системы защиты от атак, основанных на методах социотехники

Осознав всю широту спектра существующих угроз, необходимо выполнить три действия для создания системы защиты сотрудников от угроз, связанных с использованием социотехники. Помните, что эффективность защиты во многом определяется во время ее планирования. Часто защитные меры предпринимаются только после обнаружения успешно проведенной атаки для предотвращения аналогичных проблем в будущем. Этот подход показывает, что обеспечению безопасности в компании уделяется некоторое внимание, но такое решение проблемы может оказаться слишком запоздалым, если компании уже причинен значительный ущерб. Чтобы не допустить этого, нужно выполнить три следующих действия.

Разработка стратегии управления обеспечением безопасности. Определите задачи защиты от социотехнических угроз и назначьте сотрудников, отвечающих за их выполнение.

Оценка риска. В разных компаниях уровень риска, связанного с одними и теми же угрозами, может быть разным. Проанализируйте каждую из социотехнических угроз и определите, насколько она опасна для организации.

Интеграция принципов защиты от социотехнических атак в политику безопасности. Разработайте и задокументируйте политики и процедуры, регламентирующие действия сотрудников в ситуациях, которые могут оказаться социотехническими атаками. Для выполнения этого этапа необходимо, чтобы в организации уже была принята политика безопасности, охватывающая угрозы, не связанные с социотехникой. Если политика безопасности отсутствует, ее нужно разработать. Факторы, определенные на этапе оценки риска, связанного с социотехническими угрозами, помогут приступить к разработке политики безопасности, но позднее в ней нужно будет учесть и другие возможные угрозы.

Разработка стратегии управления обеспечением безопасности

Стратегия управления обеспечением безопасности должна давать общее представление о социотехнических угрозах, которым подвергается организация, и определять сотрудников, отвечающих за разработку политик и процедур, блокирующих эти угрозы. Это не означает, что на работу нужно принять специалистов, в чьи обязанности будет входить только обеспечение безопасности корпоративных активов. Такой подход возможен в крупных компаниях, но в организациях среднего размера создавать такие должности в большинстве случаев невыгодно. Главное, что нужно сделать – это распределить между некоторыми сотрудниками следующие роли.

Куратор по безопасности. Руководитель высшего звена (предположительно – уровня совета директоров), следящий за тем, чтобы все сотрудники относились к обеспечению безопасности серьезно, и обладающий необходимым для этого авторитетом.

Администратор по безопасности. Руководитель, отвечающий за организацию разработки политики безопасности и ее обновление в соответствии с изменениями требований.

Менеджер по безопасности ИТ-систем. Технический специалист, отвечающий за разработку политик и процедур обеспечения безопасности ИТ-инфраструктуры и операций.

Менеджер по безопасности на объекте. Член группы, обслуживающей здание, который отвечает за разработку политик и процедур обеспечения безопасности на объекте.

Менеджер по информированию персонала о способах обеспечения безопасности. Руководящий сотрудник (обычно из отдела кадров), отвечающий за разработку и проведение кампаний по информированию персонала об угрозах и способах защиты от них.

Сотрудники, выполняющие эти роли, формируют руководящий комитет по обеспечению безопасности (Security Steering Committee), который должен определять главные цели стратегии управления обеспечением безопасности. Если не определить эти цели, будет сложно привлекать к участию в проектах по обеспечению безопасности других сотрудников и оценивать результаты таких проектов. Первой задачей, которую должен выполнить руководящий комитет по обеспечению безопасности, является обнаружение в корпоративной среде уязвимостей, делающих возможными социотехнические атаки. Чтобы быстро получить представление о возможных векторах этих атак,

можно воспользоваться простой таблицей наподобие приведенной ниже.

Направление атаки	**Нынешнее положение дел**	**Комментарии**
Сетевые атаки		
Электронная почта	На настольных компьютерах всех пользователей установлена программа Microsoft Outlook®.	
Интернет	Мобильные пользователи в дополнение к обычному клиенту Outlook используют веб-клиент Outlook.	
Всплывающие приложения		На текущий момент никакие технические средства защиты от всплывающих приложений в компании не используются.
Служба мгновенного обмена сообщениями	Принятые в компании методики работы допускают неконтролируемое использование различных систем мгновенного обмена сообщениями.	
Телефонные атаки		
Корпоративная телефонная станция		
Служба поддержки	В настоящее время функции «службы поддержки» бессистемно выполняет ИТ-отделение.	Процессы оказания услуг поддержки нужно интегрировать в другие структуры компании.
Поиск информации в мусоре		
Внутренний мусор	Каждое отделение избавляется от собственного мусора самостоятельно.	
Внешний мусор	Мусорные контейнеры располагаются вне территории компании. Вывоз мусора осуществляется по четвергам.	На территории компании нет места для мусорных контейнеров.
Персональные подходы		
Физическая безопасность		
Безопасность офисов	Все офисы остаются незапертыми в течение всего рабочего дня.	25 процентов сотрудников работают дома. Письменные стандарты обеспечения безопасности систем сотрудников, работающих дома, отсутствуют.
Сотрудники, работающие дома	Никаких протоколов, регламентирующих обслуживание систем сотрудников, работающих дома, нет.	
Другие направления атак и уязвимости, специфические для компании		
Подрядчики, работающие на объектах компа-	Пункты питания на территории компании организованы сторонней фир-	Мы ничего не знаем о ее сотрудниках и не приняли для них по-

нии	мой.	литику безопасности.

Когда члены руководящего комитета по обеспечению безопасности основательно разберутся в имеющихся уязвимостях, они могут составить таблицу уязвимостей корпоративной среды, допускающих проведение атак, основанных на методах социотехники (см. пример выше). В этой таблице следует описать рабочие процессы компании в потенциально уязвимых областях. Информация об уязвимостях позволяет членам руководящего комитета разработать предварительные варианты требований, которые могут быть включены в политику.

Сначала руководящий комитет должен определить области, которые могут подвергнуть компанию риску. Выполняя эту задачу, нужно учесть все направления атак, описанные в данном документе, и специфические для компании элементы, такие как использование общедоступных терминалов или процедуры управления офисной средой.

Оценка риска

При разработке мер по обеспечению безопасности всегда нужно оценить уровень риска, которому подвергается компания при различных атаках. Для тщательной оценки риска не обязательно требуется очень много времени. Опираясь на информацию о главных элементах стратегии управления обеспечением безопасности, определенных руководящим комитетом по обеспечению безопасности, можно сгруппировать факторы риска в категории и назначить им приоритеты. Ниже перечислены категории риска.

- Утечка конфиденциальной информации.
- Урон репутации компании.
- Снижение работоспособности компании.
- Трата ресурсов.
- Финансовые потери.

При определении приоритета фактора риска следует учесть стоимость его устранения. Если она превышает возможный ущерб от соответствующей атаки, возможно, с риском лучше смириться. Оценка риска может предоставить очень полезную информацию на заключительных этапах разработки политики безопасности.

Например, руководящий комитет по обеспечению безопасности может обнаружить недостатки принятого в компании пропускного режима. Если предполагается, что компанию будут посещать не более 20 человек в час, будет достаточно нанять одного контролера, завести

книгу учета посетителей и пронумерованные идентификационные карточки. Если же компанию будут посещать 150 человек в час, возможно, придется расширить штат контролеров или установить терминалы для самостоятельной регистрации. В компаниях малого размера установка таких терминалов едва ли окупится, но для крупных компаний, которые в случае простоя из-за атак могут понести крупные убытки, этот вариант может оказаться наиболее эффективным.

Рассмотрим другой пример. Для компании, не принимающей посетителей и не нанимающей подрядчиков, может не быть практически никакой опасности в выкладывании распечатанных документов в одном определенном месте, откуда их будут забирать сотрудники. Между тем, для компании, часто пользующейся услугами многих подрядчиков, этот вариант связан со слишком большим риском, и ее руководители могут решить, что для предотвращения краж конфиденциальных документов из принтеров необходимо установить принтер на каждом рабочем столе. Компания может устранить этот риск, поставив условие, чтобы каждого посетителя в течение всего визита сопровождал штатный сотрудник. Это решение окажется гораздо менее дорогим, если, конечно, не учитывать финансовые следствия неэффективного использования рабочего времени сотрудников.

Используя таблицу уязвимостей корпоративной среды, допускающих проведение социотехнических атак, руководящий комитет по обеспечению безопасности может определить для компании требования политики безопасности, типы и уровни риска. При этом можно использовать следующий формат:

Направление атаки	**Возможные требования политик**	**Тип риска: утечка конфиденциальной информации, урон репутации компании, сниже-ние работоспособности компании, трата ресурсов, финансовые потери**
	Изложить политики защиты от угроз, основанных на методах социотехники, в письменной форме	
	Внести пункт о необходимости соблюдения политик в стандартный контракт с сотрудником	
	Внести пункт о необходимости соблюдения политик в стандартный контракт с подрядчиком	
Сетевые атаки		
Электронная почта	Принять политику, регламентирующую действия сотрудников при получении вложений	

	конкретных типов	
Интернет	Принять политику, регламентирующую использование Интернета	
Всплывающие приложения	Включить в политику использования Интернета явные указания по поводу того, что следует делать при появлении всплывающих диалоговых окон	
Служба мгновенного обмена сообщениями	Принять политику, определяющую поддерживаемые и допустимые клиентские программы мгновенного обмена сообщениями	
Телефонные атаки		
Корпоративная телефонная станция	Принять политику управления обслуживанием корпоративной телефонной станции	
Служба поддержки	Принять политику, регламентирующую предоставление доступа к данным	
Поиск информации в мусоре		
Бумажный мусор	Принять политику утилизации бумажного мусора	
	Определить принципы использования мусорных контейнеров	
Электронный мусор	Принять политику утилизации электронного мусора	

Сотрудники каждого подразделения будут по-разному воспринимать риск, связанный с различными угрозами. Члены комитета по обеспечению безопасности должны учесть их мнения и прийти к согласию по поводу важности разных факторов риска.

Социотехника и политики безопасности

Руководящие органы компании и представители ее ИТ-подразделения должны разработать эффективную политику безопасности и помочь реализовать ее в корпоративной среде. Иногда в политике безопасности основное внимание уделяется техническим средствам защиты, помогающим бороться с техническими же угрозами, примерами которых могут служить вирусы и черви. Эти средства ориентированы на защиту технических элементов среды, таких как файлы данных, приложения и операционные системы. Средства защиты от социотехнических угроз должны помогать отражать социотехнические атаки на сотрудников компании.

Для главных областей обеспечения безопасности и факторов риска руководящий комитет по обеспечению безопасности должен разработать документацию, регламентирующую соответствующие процедуры, процессы и бизнес-операции. В следующей таблице показано, как руководящий комитет по обеспечению безопасности с помо-

щью заинтересованных сторон может определить документы, необходимые для поддержки политики безопасности.

Требования политик	Требования к процедурам и документации	Дата выполнения действия
Изложить политики защиты от угроз, основанных на методах социотехники, в письменной форме	Отсутствуют	
Внести пункт о необходимости соблюдения политик в стандартный контракт с сотрудником	Сформулировать новые контрактные требования (юридическая служба) Определить новый формат контрактов, заключаемых с подрядчиками	
Внести пункт о необходимости соблюдения политик в стандартный контракт с подрядчиком	Сформулировать новые контрактные требования (юридическая служба) Определить новый формат контрактов, заключаемых с подрядчиками	
Принять политику работы с посетителями	Разработать процедуру регистрации посетителей при входе на объект и выходе с него Разработать процедуру сопровождения посетителей	
Определить принципы использования мусорных контейнеров	Разработать процедуру утилизации бумажного мусора (см. данные) Разработать процедуру утилизации электронного мусора (см. данные)	
Принять политику, регламентирующую предоставление доступа к данным		
Принять политику утилизации бумажного мусора		
Принять политику утилизации электронного мусора		
Включить в политику использования Интернета явные указания по поводу того, что следует делать при появлении всплывающих диалоговых окон		
Принять политику управления идентификаторами и паролями пользователей, запрещающую, например, запись паролей на клейких листках, прикрепленных к монитору, и т. д.		
Принять политику использования мобильных компьютеров вне компании		
Принять политику разрешения проблем при подключении к приложени-		

ям партнеров (таким как банковские и финансовые приложения, системы управления закупками и материально-техническими запасами)		

Как видите, такой список может оказаться в итоге довольно длинным. Чтобы ускорить его составление, можно воспользоваться помощью сторонних организаций, специализирующихся на обеспечении ИБ. Особое внимание руководящий комитет по обеспечению безопасности должен уделить приоритетным областям, определенным в ходе оценки риска.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

КАФЕДРА МОНИТОРИНГА И ПРОГНОЗИРОВАНИЯ ИНФОРМАЦИОННЫХ УГРОЗ

Заляжных В.А.
Гирик А.В.

Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел НИУ ИТМО
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Санкт-Петербургского национального
исследовательского университета
информационных технологий, механики
и оптики
197101, Санкт-Петербург, Кронверкский пр., 49