Утверждена
приказом ОАО «Самараэнерго»

От 29.03.2013 № 38

КОРПОРАТИВНАЯ ПОЛИТИКА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРОЧИХ ВИДОВ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Содержание

Перечень сокращений

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения и наводки
СЗПДн	Система защиты персональных данных
СКУД	Система контроля и управления доступом
СУБД	Система управления базой данных
СУИБ	Система управления информационной безопасностью
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

1. Введение

В данной Политике изложены основные принципы обеспечения информационной безопасности и те действия, которые необходимо предпринимать для обеспечения безопасности персональных данных и прочих видов конфиденциальной информации ОАО «Самараэнерго» (далее – Общество).

Требования по соблюдению настоящей Политики информационной безопасности должны быть включены в положения трудовых договоров, которые заключаются с работниками Общества. Требования по обеспечению информационной безопасности в соответствии с данной Политикой, с указанием конкретных мер, должны включаться в положения договоров, которые заключаются с:

- поставщиками услуг и представителями сторонних организаций, использующих информационную систему Общества, а также с третьими лицами, работающими в Обществе;
- партнерами и третьими лицами, обрабатывающими информацию от имени Общества.

2. Общие положения

Целью настоящей Политики не является детализация всех правил и мер, направленных на обеспечения информационной безопасности, а определение направлений обеспечения информационной безопасности, актуальных для Общества. Настоящая политика подлежит пересмотру не реже одного раза в годю

3. Организация информационной безопасности

За обеспечение информационной безопасности Общества отвечает Отдел технической поддержки совместно со Службой безопасности.

3.1. Участники процесса обеспечения информационной безопасности

3.1.1. Руководитель Отдела технической поддержки

Основные задачи:

- защита информационных активов Общества и его клиентов (в рамках контрактных или договорных обязательств) от случайного или намеренного уничтожения, искажения, разглашения или потери, в том числе обеспечение непрерывности деятельности;
- обеспечение выполнения требований действующего законодательства РФ по обеспечению информационной безопасности (защита персональных данных, использование криптографических средств защиты информации и т.п.);
- обеспечение информационной безопасности продуктов, услуг, процессов и технологий Общества на основании оценки рисков.

3.1.2. Руководители любого уровня

Руководитель любого уровня обязан соблюдать требования действующего законодательства РФ и внутренних документов Общества в части обеспечения информационной безопасности, в том числе и в отношениях с третьими лицами. Руководитель обеспечивает контроль соблюдения норм и правил обеспечения информационной безопасности в своем подразделении и информирует Отдел технической

поддержки о любых подозрительных событиях и (или) о нарушениях действующих правил обеспечения информационной безопасности.

3.1.3. Сотрудники, наделенные значительными техническими правами

Сотрудники, наделенные значительными техническими правами (системные администраторы, разработчики, администраторы баз данных и т.д.), должны соблюдать правила информационной безопасности и применять любые необходимые меры по конфигурации систем для обеспечения необходимого уровня информационной безопасности.

3.1.4. Работники Общества и третьи лица

Работники Общества и третьи лица должны:

- соблюдать правила информационной безопасности;
- действовать осторожно и проявлять осмотрительность в отношении любых действий, которые могут повлечь за собой снижения уровня информационной безопасности;
- информировать своих непосредственных руководителей и представителей Отдела технической поддержки обо всех подозрительных событиях информационной безопасности.

3.1.5. Ответственность в должностных обязанностях

Обязанность соблюдения правил обеспечения информационной безопасности, установленных в Обществе, любого работника Общества должна быть в обязательном порядке отражена в его должностной инструкции.

3.2. Правовое обеспечение информационной безопасности

Обеспечение информационной безопасности Общества производится в соответствии с действующим законодательством РФ, стандартами и рекомендациями ФСБ России и ФСТЭК России.

3.3. Финансовые аспекты обеспечения информационной безопасности

Должен обеспечиваться баланс между «стоимостью принимаемого риска» и «затратами на информационную безопасность». Планы действий по обеспечению информационной безопасности должны формироваться на основе анализа рисков нарушения информационной безопасности Общества. План должен определять действия по устранению неприемлемых рисков, влияющих на жизнеспособность и основные направления деятельности Общества.

Следует проводить анализ затрат на информационную безопасность и сравнивать их с последствиями реализации угроз информационной безопасности.

4. Основные правила обеспечения информационной безопасности

4.1. Управление ресурсами

В Обществе должны быть определены владельцы информационных ресурсов Общества. Ресурсы делятся на три категории: информация, программное обеспечение и материальные ценности (оборудование).

4.2. Ответственность за обеспечение информационной безопасности

Начальники подразделений должны обеспечить информирование работников и третьих лиц о правилах информационной безопасности Общества и ответственности за их нарушение.

4.3. Осведомлённость персонала в области информационной безопасности

Каждый работник Общества должен быть проинформирован о правилах информационной безопасности и знать, какие санкции могут быть к нему применены в случае несоблюдения требований информационной безопасности. Работники Общества должны получать соответствующую и постоянно обновляемую информацию о требованиях информационной безопасности и средствах контроля.

4.4. Соглашение о конфиденциальности

В соглашениях о конфиденциальности должны содержаться положения о том, что в отношении ее использования действуют определенные правила. Работники Общества и третьи лица должны подписать соглашение о конфиденциальности до того, как им предоставят доступ к информационным ресурсам Общества и конфиденциальной информации.

4.5. Физическая безопасность и безопасность на рабочем месте

Оборудование, используемое для обработки конфиденциальной информации, необходимо размещать в защищенных помещениях. Доступ к оборудованию должен быть ограничен с использованием специальных средств контроля доступа. Оборудование должно быть защищено от несанкционированного доступа, повреждений и вмешательств. Данные условия размещения должны быть обеспечены лицами, осуществляющими охрану помещений Общества. Работники Общества обязаны исключить возможность наличия на их рабочем столе документов или носителей с конфиденциальной информацией, в случае их отсутствия на рабочем месте.

Конфиденциальные документы и носители с конфиденциальной информацией следует хранить в запираемых на ключ тумбах или шкафах, а в случае отсутствия такой возможности работнику следует уведомить об этом Службу безопасности.

Запрещается хранить в открытом доступе любые конфиденциальные документы или носители в таких местах как: сетевые принтеры, места для приема пищи и т.п.

4.6. Безопасность ресурсов, используемых вне территории Общества

Оборудование, программное обеспечение и конфиденциальная информация, используемые вне территории Общества, по возможности подлежат защите на основе тех же требований информационной безопасности, которые применяются и на территории Общества. Меры, применяемые для защиты конфиденциальной информации за пределами Общества по возможности должны обеспечивать наивысший уровень информационной безопасности. К таким мерам могут относиться:

- личный контроль сотрудниками Общества конфиденциальности и целостности ресурсов;
- использование на рабочих станциях и серверах средств от несанкционированного доступа;
- уничтожение конфиденциальной информации с носителей информации при передаче оборудования на гарантийное обслуживание;
- подписание соглашения о неразглашении конфиденциальной информации с организацией, имеющей доступ к конфиденциальной информации Общества;
- другие меры направленные на обеспечение безопасности ресурсов Общества вне территории Общества.

4.7. Техническое обслуживание оборудования

Для оборудования, входящего в информационную автоматизированную систему Общества, необходимо подписывать договор на техническое обслуживание с указанием времени проведения работ по обслуживанию или гарантийной замены (например, соглашение об уровне обслуживания). Время на восстановление работоспособности системы после аварии должно соответствовать требованиям бизнес-процесса.

Техническое обслуживание системы сторонними организациями не должно приводить к риску раскрытия конфиденциальной информации. Для этого возможно применение следующих мер:

- проведение технического обслуживания оборудования в присутствии сотрудников Общества;
- подписание соглашения о неразглашении конфиденциальной информации с организацией проводящей техническое обслуживание оборудования;
- другие меры направленные на обеспечение конфиденциальности информации Общества при техническом обслуживании оборудования.

4.8. Резервирование

Резервирование заключается в наличии нескольких экземпляров запасного оборудования и программного обеспечения или нескольких комплектов запасных частей для повышения производительности и (или) для обеспечения соответствующей доступности в случае выхода из строя основного оборудования. Допустима ситуация, когда заключен договор с внешней организацией, согласно которому определен срок поставки запасного оборудования. Все информационные системы должны иметь резервные системы (горячее резервирование/кластер или холодное резервирование). Должны быть определены процедуры, обеспечивающие непрерывность бизнес-процессов, или процедуры восстановления бизнес- процессов после возникновения инцидента.

Крупные системы должны быть обеспечены, как минимум, частичным резервированием их важных подсистем (например, электропитание).

4.9. Использование носителей информации

Необходимо контролировать использование любых носителей информации, для предотвращения несанкционированного разглашения конфиденциальной информации, внесения изменений, удаления или уничтожения указанной информации, а также внесения изменений в работу информационных систем.

Должен обеспечиваться контроль и учет при использовании носителей информации.

По возможности вся информация, которая хранится на носителе, должна быть в зашифрованном виде.

Работники Общества и третьи лица должны использовать носители информации только для выполнения своих служебных обязанностей или положений договоров, заключаемых между ними и Обществом. Использование носителей в иных целях категорически запрещено.

Работникам Общества и третьим лицам запрещается использовать носители информации в информационных системах Общества без согласования со Службой безопасности.

4.10. Утилизация и передача носителей информации

Любую конфиденциальную информацию необходимо гарантированно уничтожать с носителя информации до момента его утилизации или передачи третьим лицам, за исключением случаев, когда это предусмотрено договором.

4.11. Использование сети Интернет

Работникам, а также третьим лицам, работающим на территории Общества, разрешается использовать сеть Интернет в личных целях, если это не отражается на выполнении ими своих служебных обязанностей.

При пользовании сетью Интернет в независимости от целей пользования, запрещается:
- использовать интернет в целях способных нанести вред Обществу, его репутации, иных целях, противоречащих законодательству РФ;
- посещать интернет ресурсы, содержащие порнографические, эротические материалы, в том числе любой сексуальной направленности и ориентации;
- посещать интернет ресурсы, имеющие радикальную, экстремистскую и террористическую направленность;
- скачивать любое программное обеспечение или пересылать такое, вне зависимости от того платное оно или бесплатное, в том числе исполняемые файлы. Исключительным правом обладает только Управление по информационным технологиям;
- передавать или распространять любую конфиденциальную информацию;
- использовать адрес корпоративной электронной почты при регистрации на интернет-ресурсах, только если это не определено внутренним документом Общества;
- пользоваться любой платной или бесплатной электронной почтой (www.mail.ru, www.yandex.ru, и т.п.);
- посещать интернет-ресурсы так называемых социальных сетей (www.vk.com, www.odnoklassniki.ru. www.facebook.com и т.п.);
- пользоваться любым программным обеспечением для передачи текстовой и иной информации другим пользователям сети Интернет (ICQ, и т.п.);
- пользоваться чатами и форумами, если это не определено отдельным внутренним документом Общества;
- данный список может быть дополнен.

Для целей обеспечения экономической безопасности и вопросов работы с потребителями электроэнергии, имеющими просроченную задолженность, могут допускаться исключения из правил.

Должен осуществляться мониторинг действий работников Общества или третьих лиц в сети Интернет. Данный мониторинг должен осуществляться Отделом технической поддержки.

4.12. Использование корпоративной электронной почты

Корпоративная электронная почта может использоваться работниками Общества или третьими лицами как для выполнения ими своих служебных обязанностей, так и в личных целях. Работникам Общества или третьим лицам в независимости от целей пользования запрещается:
- использовать электронную почту для отправки сообщений, содержащих угрозы, клевету, способных нанести вред Обществу, его репутации, унижающих людей по расовому или половому признаку, призывающих к свержению действующего государственного строя,

порнографические, эротические материалы, в том числе любой сексуальной направленности и ориентации;
- отправлять на внешние почтовые адреса электронные сообщения, содержащие конфиденциальную информацию, если это явно не определено внутренними документами Общества;
- отправлять сообщения, содержащие исполняемые файлы, если это не определено внутренними документами Общества;
- устанавливать пересылку с корпоративного почтового адреса или адресов на внешние почтовые адреса;
- отправлять сообщения, размер которых превышает десять мегабайт;
- осуществлять попытки несанкционированного доступа к корпоративной почте работников Общества или третьих лиц;
- данный список может быть дополнен.

Вся корпоративная электронная почта является собственностью Общества и не принадлежит работникам или третьим лицам. Работники Общества и третьи лица, использующие корпоративную электронную почту для отправки и приема почтовых сообщений в личных целях, должны понимать, что Общество имеет право обрабатывать (хранить, читать, удалять, архивировать, фильтровать, анализировать, в том числе автоматическими средствами и т.д.) корпоративную электронную почту по своему усмотрению.

Отдел технической поддержки должен осуществлять мониторинг действий работников Общества или третьих лиц при использовании корпоративной электронной почты.

4.13. Безопасность инфраструктуры

Компоненты информационных систем Общества должны иметь необходимый функционал, обеспечивающий информационную безопасность (возможность контроля, обновлений и т.д.). Все изменения в инфраструктуре информационных систем должны согласовываться с Отделом технической поддержки и Службой безопасности.

Необходимо разработать (или выбрать), оборудовать, конфигурировать и интегрировать все компоненты информационных систем таким образом, чтобы минимизировать риски нарушения информационной безопасности.

4.14. Контроль доступа

Контроль доступа к системам, приложениям и данным должен соответствовать конфиденциальности данных, к которым предоставляется доступ.

Механизмы контроля доступа нельзя игнорировать или нарушать. Для предоставления доступа пользователю к приложению, необходимо руководствоваться правилами предоставления доступа к данному приложению. Необходимо, чтобы права доступа:
- были индивидуальными, использовались для авторизации пользователя и были предоставлены ему на период его работы;
- были определены на основании формализованной процедуры;
- соответствовали принципу «минимизации полномочий» с тем, чтобы пользователям были предоставлены только те права доступа, которые им необходимы для выполнения своих служебных обязанностей;

- могли быть приостановлены или аннулированы в любой момент времени;
- постоянно пересматривались (не реже двух раз в год) для подтверждения необходимости предоставленных прав.

4.15. Безопасность пароля

Необходимо, чтобы в Обществе были определены правила создания паролей ко всем информационным системам. Пароли должны быть сложными (содержать строчные и заглавные буквы, спецсимволы, цифры), длина пароля должна быть не менее 8 символов. Все пароли во всех информационных системах должны регулярно меняться, не реже одного раза в три месяца. Количество неверных попыток ввода пароля должно быть ограничено пятью, после чего доступ должен быть заблокирован.

4.16. Управление рисками

Необходимо на регулярной основе, не реже 2 раз в год, проводить оценку рисков нарушений информационной безопасности.

4.17. Безопасность информационной сети

Необходимо гарантировать и контролировать безопасность информационной сети Общества. При определении мер обеспечения информационной безопасности информационной сети Общества необходимо исходить из требований максимального уровня защиты.

4.18. Соединения внутри информационной сети Общества

При объединении сегментов внутренней информационной сети Общества должны быть обеспечены все необходимые меры для обеспечения информационной безопасности.

Соединения:

- должны быть управляемыми в отношении информационной безопасности (контролируемый доступ, использование и т.д.);
- не должны подключаться к неавторизованным информационным сетям (WIFI, GPRS, и т.д.)

4.19. Соединение с внешними информационными сетями

Любое соединение с внешней системой или информационной сетью должно быть согласовано с Отделом технической поддержки. Любой доступ должен быть ограничен и протестирован на возможные уязвимости. Необходимо применять принцип многоуровневой защиты (несколько уровней брандмауэров, отключение протоколов и т.д.). Внешний доступ должен также отвечать следующим характеристикам:

- третьи стороны должны подписывать соглашение о взятие на себя обязательств по обеспечению информационной безопасности своей части сети, соединенной с сетью Общества, а также соглашение о неразглашении конфиденциальной информации;
- должен быть обеспечен контроль доступа и его аутентификация.

4.20. Безопасность информации

Отнесение информации к конфиденциальной должно производиться в соответствии с действующим законодательством РФ.

4.20.1. Классификация информации

Вся конфиденциальная информация, в независимости от вида защищаемой информации: коммерческая тайна, персональные данные и т.д., должна быть классифицирована по следующему принципу:

- К1 - информация доступная всем работникам Общества;
- К2 - информация, доступ к которой имеет ограниченное количество работников Общества;
- К3 - информация, доступ к которой имеют члены Руководства Общества и иные лица, список которых утвержден Руководством Общества.

Во всех документах должно в обязательном порядке указываться степень конфиденциальности, а так же какие должностные лица и структурные подразделения имеют к документу доступ. В документах, информация в которых не является конфиденциальной, никаких пометок, указывающих на открытость информации, не ставится.

Ограничительные пометки, грифы ставятся на документы в соответствии с отдельными частными политиками.

4.20.2. Использование криптографических средств защиты информации

Для обеспечения информационной безопасности Общество может использовать средства криптографической защиты информации (далее - СКЗИ) в соответствии с действующим законодательством.

Необходимость использования СКЗИ должно быть отражено в моделях угроз и моделях нарушителя.

Минимум два работника Общества должны отвечать за работу с СКЗИ, а их ответственность должна быть закреплена во внутренних документах Общества и должностных инструкциях.

4.21. Обработка персональных данных

Защита персональных данных должна быть организована как минимум следующим образом:

- персональные данные потребителей электроэнергии должны обрабатываться в минимально необходимом объеме;
- все работники Общества, задействованные в обработке персональных данных, обязаны строго соблюдать внутренние документы Общества, регламентирующие защиту персональных данных;
- в случае передачи третьим лицам персональных данных, до момента передачи, данный вопрос должен быть согласован с ответственным по защите персональных данных.;
- в Обществе должен быть разработан отдельный порядок по обработке и защите персональных данных, с указанием функций каждого структурного подразделения Общества, а также указанием конкретных мер по защите персональных данных.

5. Основные меры обеспечения информационной безопасности

5.1. Предотвращение инцидентов информационной безопасности

В Обществе должны предприниматься все возможные меры для предотвращения любых инцидентов информационной безопасности.

Для предотвращения инцидентов должны выполняться следующие меры:
- регулярный контроль и анализ трафика сети и работоспособности информационной системы;
- регулярная проверка обновлений системы, процедур и документации;
- регулярная оценка уязвимости посредством внутреннего и, при необходимости, внешнего аудитов;
- регулярная активация и проверка журналов регистрации системы и журналов по регистрации отчетов об ошибках;
- рассмотрение вопросов информационной безопасности на начальных стадиях любых проектов;
- повышение уровня осведомленности работников Общества;
- иные меры.

5.2. Мониторинг текущего уровня информационной безопасности

Мониторинг осуществляется Отделом технической поддержки. Мониторинг направлен на:
- выявление уязвимостей, которые могут привести к реализации угроз информационной безопасности;
- выявления фактов нарушения правил информационной безопасности работниками Общества, а также третьими лицами;
- определение необходимости внесения изменений в существующий порядок обеспечения информационной безопасности.

5.3. Обеспечение информационной безопасности при разработке приложений

Разработка или обновление приложения не должны быть причиной возникновения риска нарушения действующих правил информационной безопасности. Для этого должны применяться, как минимум, следующие меры безопасности:
- должна обеспечиваться конфиденциальность процесса разработки приложения или его изменения;
- должна обеспечиваться безопасность среды, в которой происходит разработка;
- необходимо обеспечить возможность проведения аудита (подтверждение того, что элементы контроля включены в проектные спецификации, и их использование может быть проверено);
- код приложения должен быть безопасен (отсутствие уязвимых мест, отсутствие возможностей кода, которые не были определены, защита от вирусов и т.п.);
- соблюдение авторских прав;
- все ошибки, которые были выявлены в момент разработки приложения, должны быть устранены до момента внедрения приложения;
- должна обеспечиваться аутентификация пользователя при последующем использовании приложения;
- приложение должно быть разработано таким образом, чтобы каждый пользователь мог выполнять только те операции, на которые у него есть полномочия в рамках своих должностных обязанностей;
- приложения должны функционировать таким образом, чтобы гарантировать, что ни одна из функций процесса не задействует больше, чем строго ограниченный минимум набора прав, требуемых для выполнения самого приложения.

Важно гарантировать, чтобы каждая функциональность приложения:
- не давала возможности приложению иметь права суперпользователя в других информационных системах;
- имела только необходимые привилегии во время выполнения;
- имела доступ только к тому, что необходимо для исполнения.

5.4. Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности Общества при взаимоотношении с третьими лицами должны обеспечиваться действующие правила и меры по обеспечению информационной безопасности, и выполняться как минимум следующие меры:
- должно заключаться соглашение о неразглашении конфиденциальной информации;
- по возможности должен проводиться мониторинг действий третьих лиц в информационных системах Общества;
- по возможности предусмотреть в договорах с третьими лицами право Общества на проведение аудита обеспечения информационной безопасности той информации, которую Общество передает третьему лицу.

В случае заключения договора с юридическим лицом, предметом которого является передача информации, принадлежащей Обществу на законных основаниях, Общество должно удостовериться до заключения договора в адекватном уровне обеспечения информационной безопасности юридического лица. Адекватным уровнем может являться: наличие аудиторского заключения независимого аудитора уровня информационной безопасности как юридического лица в целом, так и отдельного направления деятельности в частности. Обязательным является получение доказательств выполнения действующего законодательства РФ по защите персональных данных.

5.5. Информационная безопасность ИТ инфраструктуры

5.5.1. Наличие достаточных мощностей

Информационная инфраструктура Общества должна иметь достаточно мощностей для обработки и хранения информации в соответствии с требованиями Общества. Всегда должны обеспечиваться дополнительные резервные мощности на случай появления дополнительной нагрузки на информационную инфраструктуру.

5.5.2. Управление доступностью

Должна быть обеспечена доступность всех ключевых (критических для бизнеса) информационных систем. Все информационные системы и бизнес-процессы, их использующие, должны быть классифицированы по степени важности и составлен план по обеспечению их доступности.

5.5.3. Документирование процедур

Функционирование информационных систем Общества должно быть документально оформлено актом ввода в эксплуатацию и эксплуатационной документацией, в том числе и на бумажном носителе со сроком хранения не менее 5 лет.

Любые изменения в информационных системах также должны быть документально оформлены.

5.5.4. Обеспечение непрерывности деятельности

В Обществе должен быть разработан план обеспечения непрерывности деятельности, в том числе должно быть обеспечено резервирование действующего центра обработки данных. План должен регулярно (не реже двух раз в календарный год) тестироваться.

5.5.5. Использование антивирусных средств защиты

Для предупреждения, обнаружения и устранения вредоносных кодов (компьютерных вирусов, «червей», «троянских коней», логических бомб, шпионских ПО и т.д.) необходимо применение следующих мер:

- в Обществе должно использоваться на постоянной основе антивирусное средства защиты;
- информация, обрабатываемая в информационных системах Общества должна на регулярной основе проверяться антивирусным сканированием на наличие вредоносных кодов, в том числе при использовании носителей информации;
- сигнатурные базы вирусов и антивирусные средства защиты необходимо регулярно обновлять. Должна существовать процедура для быстрых обновлений в исключительных случаях при возникновении вирусной эпидемии;
- пользователи не должны иметь возможность доступа к конфигурации антивирусного средства защиты или функциям его деактивации;
- необходимо определить процедуру для обработки/восстановления инфицированных данных и, по возможности отслеживания источника заражения;
- иные меры.

5.5.6. Управление изменениями

Все изменения в информационных системах Общества должны производиться с учетом требований по информационной безопасности, и с этой целью:

- предварительно тестироваться, а в ряде случаев проходить аудит до внедрения;
- не приводить к каким-либо нарушениям в обслуживании;
- быть отслеживаемыми и документально оформленными;
- должна быть обеспечена возможность возврата к предыдущему состоянию, а в случае отсутствия такой возможности такое изменения должно быть дополнительно протестировано.

5.5.7. Разделение сред обработки информации

Продуктивная среда обработки информации должна быть отделена от среды тестирования. Необходимо строго соблюдать данное разделение для аппаратных средств, систем, приложений, баз данных и профилей доступа пользователей. Количество конфиденциальной информации в среде тестирования должно быть минимально, а в ряде случаев должно быть исключено. Тестовая среда должна полностью соответствовать продуктивной среде в части объема и количества выполняемых задач.

5.5.8. Контроль за работой информационных систем

Должны обеспечиваться следующие меры контроля:

- наблюдение в реальном времени с помощью систем обнаружения вторжений за отклонениями и подозрительными событиями в информационных системах, которые,

например, могут относиться к попыткам несанкционированного проникновения в информационные системы;
- должен регулярно проводиться анализ журналов регистрации инцидентов информационной безопасности;
- должен проводиться мониторинг производительности информационных систем для обнаружения отклонений или несоблюдения установленных требований.

5.5.9. Аудит информационных систем

Для всех информационных систем и приложений необходимо проводить аудит с точки зрения информационной безопасности. Аудит должен проводиться на регулярной основе. Аудит может проводиться сотрудниками Общества или сторонней организацией. Целью такого аудита является выявление любых событий, влияющий на текущий уровень информационной безопасности (остановка сервиса, отклонения, нарушения установленных лимитов, изменения в конфигурации, незаконное присвоение прав и т.д.).

В рамках аудита информационных систем также должны проверяться программные и аппаратные средства на предмет соблюдения установленных правил информационной безопасности. Эти проверки должны охватывать, как минимум: общую конфигурацию, обзор истории событий, обзор профилей авторизации и контроль обновлений и настроек и т.п.

Результаты аудитов должны быть документально оформлены и доведены до руководства Общества, также должно быть обеспечено их хранение не менее 5 лет, как в электронном виде, так и на бумажных носителях.