ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Роли и ответственность субъектов

Федоров Дмитрий Николаевич
dnf@dnf.su

VIII

РАЗДЕЛЫ ТЕМЫ

- Субъекты информационного пространства
- Принципы распределения прав и ответственности
- Упрощенная модель классификации субъектов
- Полная модель классификации субъектов
- Сопоставление ролей классам обрабатываемой информации
- Результаты классификации информационных систем

Раздел 1

СУБЪЕКТЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

ПОНЯТИЕ СУБЪЕКТА

- Под субъектом информационного пространства будем понимать людей, процессы или средства работы с информацией, выполняющие в информационном пространстве некие активные действия в отношении информационной системы.
- Процессы и средства как безличные сущности могут выполнять свои действия:
  - либо от имени пользователей, управляющих ими в данный момент времени, — в этом случае они будут рассматриваться неотделимо от человека и его профиля прав и ответственности;
  - либо как независимые субъекты системы с собственными профилями прав доступа.

РАМКИ КЛАССИФИКАЦИИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

- Следует различать классификацию субъектов в рамках всего информационного пространства предприятия и в рамках конкретной информационной системы.
- Хотя эти классификации могут и совпадать, но обычно они различаются, так как классификация в конкретной информационной системе носит более производственно-ориентированный характер, чем в первом случае.
- Например, с точки зрения конкретной системы пользователи, выполняющие транзакции вида 1, и пользователи, выполняющие транзакции вида 2, — это две различные группы пользователей, в то время как для информационного пространства в целом обе эти группы — это субъекты, работающие с одним объектом, база данных транзакций.

Раздел 2

ПРИНЦИПЫ РАСПРЕДЕЛЕНИЯ ПРАВ И ОТВЕТСТВЕННОСТИ

ФУНДАМЕНТАЛЬНЫЕ ПРИНЦИПЫ РАСПРЕДЕЛЕНИЯ РОЛЕЙ И ОТВЕТСТВЕННОСТИ

1. Распределение ответственности (англ. separation of duties)
   - Этот принцип означает, что в системе (пространстве) не должно быть субъекта, который мог бы самостоятельно от начала до конца выполнить операцию, которая может нанести ущерб безопасности.
2. Минимизация привилегий (англ. least privelegies).
   - Этот принцип означает, что пользователю предоставляется ровно столько прав, сколько ему необходимо для выполнения работы

РЕШЕНИЯ ДЛЯ «РАСПРЕДЕЛЕНИЯ ОТВЕТСТВЕННОСТЕЙ»

- Если пользователь А выполняет некую транзакцию, имеющую существенное значение для системы, то она должна вступить в силу только после того, как пользователь Б проверит и подтвердит ее корректность (один - формирует данные, другой — только авторизует).
- Если конкретная операция в системе не может быть разделена между двумя пользователями, значит, при ее критической важности, она должна быть выполнена одним пользователем только в присутствии другого. Это может быть достигнуто, например, разделением пароля на аутентификацию пользователя, от имени которого запускается функция, на две (или более) части. Иногда можно встретить другое определение такого принципа — "в четыре глаза" (англ. four eyes).
- Если же объективно ряд значимых операций должен выполняться только одним человеком, то результаты его действий должны регистрироваться в журналах, к которым он не имеет доступа на корректировку. Эти журналы должны регулярно анализироваться другим человеком.

РЕШЕНИЯ ДЛЯ «МИНИМИЗАЦИИ ПРИВЕЛЕГИЙ»

- Если в обязанности пользователя входит формирование отчетов по всей базе данных, то он должен иметь доступ ко всем данным, но только на чтение.
- Если пользователь должен выполнять транзакции, изменяющие состояние двух групп объектов, то он должен иметь доступ на модификацию (в зависимости от конкретной задачи, возможно, на создание и/или удаление) только к этим двум объектам.
- Объективно в информационном пространстве должен присутствовать субъект, имеющий полный доступ ко всем ресурсам, хотя бы для того, чтобы добавлять новых пользователей и наделять их правами на доступ (а значит, и имеющий возможность установить себе полный доступ ко всем информационным объектам) — например, администратор локальной сети.
- Возможно, это будет верно для небольших предприятий, однако там, где есть возможность содержать в штате более одного администратора, необходимо разделять их права, например, с помощью выделения доменов ответственности, на ресурсном принципе или по какой-либо другой схеме.

РОЛИ

- Набор прав и обязанностей, который можно применить к тому или иному сотруднику в зависимости от его функций, называется ролью.
- Цель политики ролей на предприятии — унифицировать и упростить делегирование прав сотрудникам.
- После разработки подобной схемы исчезает необходимость составлять ради каждого вновь прибывшего работника набор его прав и обязанностей и настраивать сотни учетных записей. Достаточно указать принадлежность сотрудника той или иной роли, и, возможно, произвести минимальное редактирование профиля.

Раздел 3

УПРОЩЕННАЯ МОДУЛЬ КЛАССИФИКАЦИИ СУБЪЕКТОВ

СУБЪЕКТЫ

- В информационном пространстве предприятия существуют следующие субъекты:
  - создающие объекты;
  - использующие объекты;
  - администрирующие объекты (то есть обеспечивающие среду работы с объектами других субъектов);
  - контролирующие использование объектов субъектами.
- Каждый конкретный субъект может совмещать в себе несколько или все указанные классификационные сущности.

ГРУППЫ ПО СПОСОБАМ РАБОТЫ С ИНФОРМАЦИЕЙ

- Группа А. Один субъект владеет информацией, самостоятельно обрабатывает ее без передачи другим субъектам. В этом случае он сам контролирует все способы работы и классификацию информации.
- Группа Б. Один субъект владеет информацией и передает ее для использования другому субъекту или группе субъектов. При этом он должен произвести классификацию информации, определить правила ее использования и ознакомить с ними пользователей, либо уполномочить другого субъекта (или нескольких субъектов) на выполнение этих действий.
- Группа В. Группа субъектов использует один и тот же информационный объект (в целом или различные его части) или совокупность объектов без явно выраженного права владения одним субъектом.
  - В этом случае необходимо произвести разделение субъектов на пользователей, администраторов и контролеров
- Группа Г. Субъект или группа субъектов использует информацию, владелец которой находится вне организации. В этом случае субъекты следуют правилам использования информации, определенной владельцем в рамках законодательного пространства.
- Группа Д. Группа субъектов использует информационные объекты широкого или неопределенного доступа. В этом случае работа с объектами производится без ограничений, в рамках законодательного пространства.

ОБЯЗАННОСТИ СУБЪЕКТОВ ПО ЖИЗНЕННЫМ СТАДИЯМ ИНФОРМАЦИИ

- Субъекты-Контролеры должны разработать (и при необходимости дорабатывать) правила, по которым пользователи будут работать с объектами. Кроме того, они должны произвести классификацию информационных объектов, обеспечить ознакомление пользователей с правилами и классификацией, а также контролировать соблюдение этих правил.
- Субъекты-Администраторы должны обеспечить наличие условий для создания, использования, передачи и хранения объектов в соответствии с задачами, определяемыми уполномоченными субъектами-пользователями (далее пользователями), а также создать условия для осуществления контроля со стороны субъектов-контролеров за действиями как пользователей, так и администраторов. В своей работе администраторы должны следовать разработанным правилам.
- Пользователи должны работать с объектами в соответствии с бизнес-задачей в рамках разработанных правил

Раздел 4

ПОЛНАЯ МОДЕЛЬ КЛАССИФИКАЦИИ СУБЪЕКТОВ

СУБЪЕКТЫ ПОЛНОЙ МОДЕЛИ

Сложная западная модель, предложенная в книге «Handbook of Information Security Management» («Руководство по управлению информационной безопасности»).

- Владелец информации
- Хранитель информации
- Владелец приложения
- Администратор пользователей
- Администратор безопасности
- Аналитик безопасности
- Аналитик контроля модификаций
- Аналитик данных
- Провайдер (поставщик) решений
- Конечный пользователь
- Владелец процесса
- Администратор продукта

Не все субъекты могут быть актуальны для средних и малых компаний

ВЛАДЕЛЕЦ ИНФОРМАЦИИ

Владелец информации — бизнес-менеджер, который ответственен за информационные активы предприятия.

Обязанности следующие:

- устанавливать первичную классификацию информации и периодически проверять, что эта классификация отвечает производственным задачам;
- определять работу механизмов безопасности в соответствии с классификацией;
- анализировать актуальность прав доступа к информационным активам;
- определение требований безопасности, резервного копирования и критериев доступа к информационным активам;
- выполнять или назначать исполнителей для следующих операций:
  - санкционирование запросов на доступ от других бизнес-подразделений;
  - резервное копирование;
  - восстановление данных;
- санкционировать различные действия по фактам нарушения безопасности.

ХРАНИТЕЛЬ ИНФОРМАЦИИ

Хранитель информации — обычно специалист по информационным технологиям, основная задача которого — резервное копирование и восстановление данных.

Обязанности следующие:

- производить резервное копирование в соответствии с требованиями, установленными владельцем информации;
- при необходимости восстанавливать потерянные или поврежденные данные;
- производить необходимые мероприятия по обеспечению сохранности и доступности данных из резервных копий;
- обеспечивать учет хранения в соответствии с требованиями владельца информации.

ВЛАДЕЛЕЦ ПРИЛОЖЕНИЯ

Владелец приложения — руководитель бизнес-подразделения, который полностью ответственен за выполнение производственных или иных функций, обслуживаемых приложением. Имеет следующие обязанности:

- устанавливать критерии доступа пользователей и требования к доступности для приложения;
- контролировать адекватность использования механизмов безопасности приложения (то есть, если информация, скажем, "совершенно секретная", то и механизм безопасности не может быть таким же, как для просто "секретной" информации);
- исполнять или поручать исполнение следующего:
  - ежедневное администрирование безопасности;
  - рассмотрение отдельных запросов на доступ;
  - анализ случаев нарушения безопасности;
  - рассмотрение и утверждение всех изменений к приложению до их установки на реальную систему;
  - подтверждение актуальности прав доступа пользователей в рамках приложения.

АДМИНИСТРАТОР ПОЛЬЗОВАТЕЛЕЙ

Администратор пользователей — непосредственный руководитель сотрудников. В его полной ответственности — учетные данные пользователей и информационные ресурсы работников предприятия (то есть системы, приложения, данные и т. п.). Администратор пользователей обычно отвечает за привлечение сторонних организаций.

Обязанности:

- информировать администратора безопасности об увольнении пользователя для удаления учетных записей пользователя, их отключения или временного блокирования;
- информировать администратора безопасности о служебных перемещениях пользователей, если это влечет изменение форм или прав доступа;
- докладывать в службу информационной безопасности обо всех происшествиях по безопасности или подозрении на такие происшествия;
- контролировать актуальность пользовательской учетной информации;
- формировать и предоставлять первичные пароли для новых пользователей;
- проводить обучение пользователей в вопросах политики безопасности, ее процедурам, стандартам и т. п.

АДМИНИСТРАТОР БЕЗОПАСНОСТИ

Администратор безопасности — сотрудник предприятия, который имеет соответствующие полномочия в системе управления доступом. Он устанавливает механизмы безопасности, администрирует учетные записи пользователей и права доступа к информационным ресурсам. Он подотчетен либо бизнес-подразделению, либо службе информационной безопасности внутри подразделения информационных технологий. Имеет следующие обязанности:

- разбираться в различных средах обработки данных и в результатах предоставления доступа к ним;
- контролировать тот факт, что запросы на доступ соответствуют общей линии использования информации и правилам безопасности;
- администрировать права доступа в соответствии с критериями, установленными владельцем информации;
- создавать и удалять учетные записи пользователей, установленные администратором пользователей;
- администрировать систему в рамках своей работы и функциональных обязанностей;
- расследовать отчеты о нарушениях безопасности;
- направлять начальные пароли новых пользователей только непосредственным начальникам этих пользователей.

АНАЛИТИК БЕЗОПАСНОСТИ

Аналитик безопасности — сотрудник, ответственный за определение развития безопасности данных (стратегий, процедур, правил) для обеспечения уверенности в том, что контроль и защита информации основаны на значимости информации, риске потери или компрометации и легкости восстановления. Обязанности:

- предоставлять руководства по безопасности для процедур управления информацией;
- обеспечивать понимание основных принципов работы с информацией, для того чтобы убедиться, что используются соответствующие механизмы контроля;
- обеспечивать участие, консультации и анализ в разработке систем защиты данных.

АНАЛИТИК КОНТРОЛЯ МОДИФИКАЦИЙ

Аналитик контроля модификаций — сотрудник, ответственный за анализ запросов на модификацию инфраструктуры информационных технологий и определение влияния этих изменений на работу приложений.

АНАЛИТИК ДАННЫХ

Аналитик данных — этот сотрудник анализирует бизнес-требования к разработке структур данных, рекомендует определение стандартов данных и физические платформы для них. Он ответственен за применение соответствующих стандартов управления данными. Обязанности:

- разрабатывать структуру данных для соответствия потребностям бизнеса;
- разрабатывать физическую структуру баз данных;
- создавать и поддерживать логические модели данных на основе бизнес-требований;
- обеспечивать техническую поддержку владельцу информации в разработке архитектуры данных;
- записывать метаданные (сведения о хранении данных) в библиотеку данных;
- создавать, поддерживать и использовать метаданные для эффективного управления распределением данных.

ПРОВАЙДЕР РЕШЕНИЙ

Провайдер (поставщик) решений — сотрудник, участвующий в разработке решений (приложений) и процессе разворачивания бизнес-решений. В различных информационных системах называется интегратором, разработчиком приложений, провайдером информационных технологий. Обязанности:

- работать с аналитиком данных для обеспечения уверенности, что приложение и данные будут работать совместно в соответствии с бизнес-требованиями;
- передавать технические требования аналитику данных для обеспечения соответствия требований производительности и отчетности.

КОНЕЧНЫЙ ПОЛЬЗОВАТЕЛЬ

Конечный пользователь — любой сотрудник, контрактник или поставщик предприятия, использующий информационные системы и ресурсы в рамках своей работы. Обязанности:

- сохранять в тайне пароли на доступ;
- осознавать, что безопасность информации — это в том числе и его забота;
- использовать бизнес-активы и информационные ресурсы предприятия только для целей, определенных руководством;
- соблюдать все аспекты политики безопасности, процедур, стандартов и руководств по информационной безопасности;
- по запросу предоставлять руководству отчеты по событиям, связанным с информационной безопасностью.

ВЛАДЕЛЕЦ ПРОЦЕССА

Владелец процесса — сотрудник, ответственный за внедрение, управление и постоянное улучшение процесса, соответствующего определенной потребности производства.

Обязанности:

- контролировать требования к данным, которые должны быть направлены на поддержку бизнес-процесса;
- понимать, как доступность и качество влияют на эффективность процесса;
- работать совместно с владельцем информации для определения и отстаивания программы качества данных внутри процесса;
- разрешать проблемы с данными в рамках приложения внутри процесса.

АДМИНИСТРАТОР ПРОДУКТЫ

Администратор продукта — сотрудник, ответственный за понимание бизнес-требований и формулирование их в виде требований к продукту, за работу с поставщиком и пользователями для обеспечения соответствия продукта этим требованиям, за отслеживание новых версий и за контакты с ключевыми фигурами по вопросам приобретения новых версий. Обязанности:

- обеспечивать оценку новых версий и обновлений, планируемых для внедрения, и качественное их внедрение;
- обеспечивать соответствие программного обеспечения лицензионным соглашениям;
- отслеживать производительность продукта в соответствии с требованиями производства;
- анализировать использование, тенденции и возможности продукта для определения действий, обеспечивающих соответствие требованиям проекта по продукту.

СОПОСТАВЛЕНИЕ РОЛЕЙ ФУНКЦИОНАЛЬНЫМ ОБЯЗАННОСТЯМ ГРУППЫ СУБЪЕКТОВ В0

Примерный вид матрицы распределения доступа по узкому кругу функциональных обязанностей для сотрудников типовой организации

Объекты Субъекты	Права и профили	Электронный документ	Флаг "ОК" (ЭЦП)	Регистрационный журнал
Система (ПО)	Полный доступ	Полный доступ	Полный доступ	Полный доступ
Администратор системы	Полный доступ	Нет доступа	Нет доступа	Чтение Удаление
Администратор безопасности	Чтение	Чтение	Чтение	Чтение
Пользователь 1	Нет доступа	Создание	Чтение	Нет доступа
Пользователь 2	Нет доступа	Чтение	Создание	Нет доступа
Начальник отдела	Нет доступа	Чтение	Чтение	Нет доступа
Таблица 1. Пример матрицы распределения доступа к объектам				

ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ СУБЪЕКТОВ

- Администратор системы настраивает права доступа остальных субъектов. Он имеет доступ к регистрационному журналу для трассировки значимых событий. При определенных условиях (например, переполнение пространства хранения) администратор системы может удалить журнал, но это будет сигналом об опасном событии для администратора безопасности. Формально администратор системы может дать себе права и на документ и т. п., но это также контролируется администратором безопасности путем просмотра настроек прав и регистрационного журнала.
- Администратор безопасности (Контролер) имеет доступ ко всем параметрам — но только на чтение. Таким образом, с одной стороны, он может контролировать все изменения на предмет их авторизованности (в том числе и в документах — с точки зрения бизнес-логики), но, с другой стороны, не может вмешаться в функционирование системы.
- Пользователь 1-го уровня доступа может создать электронный документ, но не может придать ему статуса актуальности, путем выставления флага "ОК" (или придать юридическую значимость установкой электронно-цифровой подписи — ЭЦП). При этом он может просмотреть, какие из созданных им документов уже актуализированы.
- Пользователь 2-го уровня доступа не может сам создать документ, однако уполномочен придать документу статус актуальности после его просмотра и проверки корректности формирования.
- Начальник отдела контролирует оба уровня пользователей (корректность формирования документа и своевременность его актуализации) и использует готовый документ в бизнес-целях (например, отсылает его руководству или партнерам).

СОПОСТАВЛЕНИЕ РОЛЕЙ КЛАССАМ ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ

- Важна ДОСТОВЕРНОСТЬ: Д0, Д1, Д2, Д3, Д4, Д5
- Важна ЦЕЛОСТНОСТЬ: Ц0, Ц1, Ц2, Ц3, Ц4
- Важная КОНФИДЕНЦИАЛЬНОСТЬ: К1, К2, К3, К4, К5

Классы категории: "Д" означает "доступность", "Ц" — "целостность«, "К" — "конфиденциальность", цифры возрастают с убыванием значимости критерия).

ДЛЯ ОБЪЕКТОВ УРОВНЯ Д0

- Администраторы. Обязательное географически распределенное хранение объекта (кластеризация, зеркалирование и т. п.), а также ежедневное резервное копирование на внешний носитель. Санкционированную возможность управления доступом к объекту должны иметь не более двух администраторов, при этом следует обеспечить возможность аварийного администрирования объекта в случае отсутствия администраторов. Администраторы должны иметь широко известные средства коммуникационного контакта и возможность оперативного оповещения в случае сбоя в работе объекта. Доступ к внешнему носителю с резервной копии должен быть физически ограничен. Число субъектов, имеющих право доступа, не может превышать пяти. Факты использования резервной копии подлежат регистрации, так же как и все действия по управлению объектом.
- Контролеры. Необходимо определить строгие и однозначные правила работы с объектом, процедуры для осуществления контроля и способы реакции на нарушения в работе объекта. Контроль действий должен производиться не реже одного раза в рабочий день. Предусматривается создание аварийных планов на случай временной или полной недоступности объекта.
- Пользователи. Должны строго придерживаться правил работы с объектом, не пытаясь получать доступ к другим объектам, кроме предназначенного для них в соответствии с их функциональными обязанностями. При невозможности получения доступа к объекту им следует немедленно обратиться к администратору.

ДЛЯ ОБЪЕКТОВ УРОВНЯ Д1

- Администраторы. Обязательное резервное копирование объекта на жесткий диск не реже трех раз в день и ежедневное копирование его на внешний носитель. Наличие холодного резервирования средств хранения и обработки информации. Санкционированную возможность управления доступом к объекту должны иметь не более двух администраторов, при этом должна быть обеспечена возможность аварийного администрирования объекта в случае отсутствия администраторов. Администраторам надлежит иметь широко известные средства коммуникационного контакта, а пользователям — возможность оперативного оповещения их в случае сбоя в работе объекта. Доступ к внешнему носителю с резервной копией должен быть физически контролируем, случаи использования резервной копии следует регистрировать. Все действия по управлению объектом также должны регистрироваться.
- Контролеры. Необходимо разработать строгие и однозначные правила работы с объектом, процедуры для осуществления контроля и способы реакции на нарушения в действиях объекта. Контроль действий производится не реже одного раза в рабочий день. Должны быть разработаны аварийные планы на случай временной или полной недоступности объекта.
- Пользователи. Обязаны строго придерживаться правил работы с объектом, не пытаясь получать доступ к объектам помимо прав, определенных для них в соответствии с функциональными обязанностями. При невозможности получения доступа к объекту немедленно обратиться к администратору.

ДЛЯ ОБЪЕКТОВ УРОВНЯ Д2

- Администраторы. Обязательное ежедневное резервное копирование на внешний носитель. Санкционированную возможность управления доступом к объекту должны иметь не более трех пользователей. Необходимо определить одного администратора. Следует обеспечить возможность аварийного администрирования. Доступ к внешнему носителю с резервной копией должен контролироваться. Действия по изменению размещения объекта или правил доступа к объекту подлежат регистрации.
- Контролеры. Предусмотрены процедуры для осуществления контроля. Контроль действий должен производиться не реже одного раза в неделю.
- Пользователи. Должны придерживаться правил работы с объектом, не пытаясь получать доступ к другому объекту, помимо определенного для них в соответствии с их функциональными обязанностями. При невозможности получения доступа к объекту следует обратиться к администратору или пользователям, управляющим доступом.

ДЛЯ ОБЪЕКТОВ УРОВНЕЙ Д3…Д5

- Для объектов уровня Д3.
  - Работа с полезной информацией оставляется на усмотрение пользователей информации.
- Для объектов уровня Д4.
  - Работа с несущественной информацией не регламентируется.
- Для объектов уровня Д5.
  - Администраторы. Необходимо обеспечить доступными средствами ограничение попадания информации данного класса пользователям. Контролеры. Необходимо наличие регламента использования такой информации и процедур контроля за расходом пользователями ресурсов на информацию данного класса.
  - Пользователи. При обнаружении подобной информации пользователь должен принять меры к ее уничтожению и сообщить об этом администратору или контролеру.

ДЛЯ ОБЪЕКТОВ УРОВНЯ Ц0 И Ц1

- Администраторы. Необходимо обеспечить право на модификацию только для авторизованных, идентифицируемых пользователей по предъявлению пароля. Предусматривается разделение прав на модификацию данных (внесение изменения/авторизация изменения) и ведение регистрационного журнала изменений. Для хранения и обработки объектов класса ЦО предпочтительно использовать средства хранения, не включенные в общую компьютерную сеть.
- Контролеры. Следует разработать строгие и однозначные правила модификации объекта, процедуры для осуществления контроля и способы реакции на несанкционированные модификации объекта. Проверка регистрационного журнала изменений должна осуществляться не реже одного раза в рабочий день.
- Пользователи. Обязаны, с одной стороны, придерживаться правил работы с объектом, не пытаясь модифицировать объект вне рамок своих функциональных обязанностей, сохранять в тайне пароль на модификацию и не пытаться получить доступ к чужим паролям. С другой стороны, они должны осуществлять санкционированные модификации в соответствии с временным графиком и в рамках своих полномочий. На каждую модификацию информации данной категории должен быть документ в виде твердой копии соответствующей формы. При обнаружении модификации объекта, подозрительно похожей на несанкционированную, обязаны немедленно сообщить контролеру.

ДЛЯ ОБЪЕКТОВ УРОВНЯ Ц2

- Администраторы. Должны обеспечить права на модификацию только для авторизованных, идентифицируемых пользователей по предъявлению пароля. Заполнять регистрационный журнал изменений.
- Контролеры. Следует разработать правила модификации объекта, процедуры для осуществления контроля и способы реакции на несанкционированные модификации объекта. Проверка регистрационного журнала изменений должна осуществляться не реже двух раз в неделю.
- Пользователи. Должны, с одной стороны, строго придерживаться правил работы с объектом, не пытаясь модифицировать объект вне рамок своих функциональных обязанностей, сохранять в тайне пароль на модификацию и не пытаться получить доступ к чужим паролям. С другой стороны, пользователи должны осуществлять санкционированные модификации строго в соответствии с временным графиком и в рамках своих полномочий. При обнаружении модификации объекта, подозрительно похожей на несанкционированную, немедленно сообщить контролеру.

ДЛЯ ОБЪЕКТОВ УРОВНЕЙ Ц3…Ц4

- Для объектов уровня Ц3.
  - Определение способов работы с объектами данного класса оставлено на усмотрение пользователей объекта.
- Для объектов уровня Ц4.
  - Определение способов работы с объектами данного класса не регламентируется.

ДЛЯ ОБЪЕКТОВ УРОВНЕЙ К0…К1

- Для объектов уровня КО.
  - Запрещено хранение объектов данного типа в электронном виде. Необходимо обеспечить подписание пользователями объекта обязательства о неразглашении информации.
- Для объектов уровня К1.
  - Работа с объектами данного типа возможна только на отдельно стоящих компьютерах или гарантированно защищенных от удаленного доступа.
  - В этом случае пользователь информации является одновременно ее администратором и контролером, предоставляя ее для использования другим пользователям только в личном присутствии и под личным контролем. Необходимо обеспечить подписание пользователями обязательства о неразглашении информации.

ДЛЯ ОБЪЕКТОВ УРОВНЯ К2

- Администраторы. Право на ознакомление с информацией предоставляется только авторизованным, идентифицируемым пользователям по предъявлению пароля и/или ключа на внешнем носителе. Необходимо заполнять регистрационный журнал доступа.
- Контролеры. Следует разработать правила использования объекта, процедуры для осуществления контроля. Проверка регистрационного журнала изменений доступа должна осуществляться не реже одного раза в день. Необходимо обеспечить подписание пользователями обязательства о неразглашении информации.
- Пользователи. Должны строго придерживаться правил работы с объектом, не пытаясь использовать объект вне рамок своих функциональных обязанностей, сохранять в тайне пароль на доступ и не пытаться получить доступ к чужим паролям.

ДЛЯ ОБЪЕКТОВ УРОВНЕЙ К3…К5

- Для объектов уровня К3.
  - В зависимости от специфики конкретной информации используются те же требования, что и для объектов уровня К2 или К4.
- Для объектов уровня К4.
  - Определение способов работы с объектами данного класса возложено на пользователей объекта.
- Для объектов уровня К5.
  - Определение способов работы с объектами данного класса не регламентируется.

Раздел 5

РЕЗУЛЬТАТЫ КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

"КЛАССИФИКАТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ"

- В результате произведенной классификации информационной системы в службе безопасности предприятия должен появиться документ "Классификатор информационной безопасности", содержащий следующие разделы:
  - классификатор объектов;
  - классификатор средств;
  - классификатор субъектов;
  - матрица разрешений, производящая сопоставление классов объектов с классами средств их обработки и классами субъектов, выполняющих эту обработку.
- Весьма желательным дополнением к классификатору является наличие полного и актуального списка кадрового состава предприятия, к каждой строке которого добавлено поле "класс субъекта".

ИЗМЕНЕНИЕ СОДЕРЖАНИЯ КЛАССИФИКАТОРА

- Первый раздел классификатора (посвященный информационным объектам) подвергается обновлению с появлением каждого нового типа обрабатываемой информации.
- Третий раздел модифицируется в случае введения качественно новых (в плане работы с информацией) должностей на предприятии.
- Второй и особенно четвертый разделы при правильном построении классификатора практически не должны претерпевать изменений. Как уже было отмечено, список кадрового состава должен обновляться незамедлительно по факту реальных перестановок в персонале и в идеальном случае стать образующим компонентом централизованной системы распределения ключей на предприятии.
- Утверждение или хотя бы согласование "Классификатора информационной безопасности" должно производиться на уровне руководства предприятия.

Все материалы курса доступны для зарегистрированных пользователей Академии современных инфокоммуникационных технологий «АСИКТ»
www.acikt.ru