CONTROL AND PROTECTION OF INFORMATION IN THE COMPANY

КОНТРОЛЬ И ЗАЩИТА ИНФОРМАЦИИ В КОМПАНИИ

Шишманов Красимир
Доктор экономических наук, профессор
Экономическая Академия имени Д.А.Ценова (Свиштов, Болгария)
e-mail: k.shishmanov@uni-svishtov.bg

Abstract
The control and protection of the information is expressed in the possibility for an information system of the organization to ensure during the implementation of activities, its normal functioning, preventing events, expression of data in the products, modification or loss of data that represents some value for it. Read, due to the reason for these events, accidental actions or changes may be taken, which result in non-compliance with labor discipline, low qualification of the staff or the provided unauthorized access to the system.

Keywords: *information security, protection of information, control and protection of the information, protection of information system.*

JEL Classification: *D81, P47, C45*

ВВЕДЕНИЕ

Системы контроля и защиты информации от физического уничтожения или несанкционированного доступа к ней имеют первостепенное значение для информационной системы любой организации, независимо от области ее применения. Главной особенностью защищаемой информации являются ограничения, которые организация накладывает на ее распространение и использование.

Процессы, происходящие в современных организациях, можно отнести к очень сложным и высокотехнологичным. Они включают в себя различные действия по обработке и обмену информацией, отклонение которых от заранее заданного функционального алгоритма приведет к значительным потерям или невозможности дальнейшего функционирования. Параметры ответственных технологических процессов касаются контроля входящих потоков информации, хранения результатов и выработки управленческих решений. Для обеспечения их готовности и безопасности предъявляются особые требования к способу контроля и защиты информационных, административных, управленческих и коммуникационных ресурсов.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Современное функционирование корпоративных систем предполагает большое количество разнообразных средств, методов и форм сбора, обработки и передачи информации, что значительно увеличивает их уязвимость. Основными факторами в этом отношении являются:

- ✓ резкое увеличение объема информации, которая собирается, обрабатывается при исполнении служебных обязанностей;
- ✓ необходимость хранить и обрабатывать информацию разного назначения и разной принадлежности;

- ✓ увеличение количества используемых технических средств (в том числе мобильных) и усложнение взаимосвязей между ними в процессе работы;
- ✓ усложнение организации работы и технологии взаимодействия отдельных сотрудников;
- ✓ резкое расширение круга пользователей, имеющих прямой доступ к ресурсам корпоративной информационной системы;
- ✓ увеличение и усложнение обмена данными между отдельными пользователями, в том числе на больших расстояниях.

Защищенная информация используется корпорацией и различными другими системами. При этом у защищаемой информации есть свои особенности:

- Есть возможность ограничить доступ к ней. Доступ к корпоративной информации должны иметь только отдельные сотрудники или специально уполномоченные лица;
- Чем важнее информация, тем серьезнее ее защита. В зависимости от ее ценности и важности, определяются и различные степени доступа и секретности;
- Защищенная информация должна приносить пользу ее владельцу и оправдывать затраты на ее защиту.

Опасения по поводу правильного функционирования системы существуют в трех направлениях. Первое – возможность изменения или уничтожения (частично или полностью) данных (т.е. нарушение их физической целостности), второе – неправильное использование данных и нарушение последующих технологических процессов, третье – возможность несанкционированного предоставления информации, т.е. утечка информации.

Физическая потеря данных в информационных системах во многом зависит от технологии обслуживания. В этом отношении наиболее сильное негативное влияние оказывает низкая квалификация некоторых сотрудников и отсутствие достаточных знаний в области компьютерной обработки данных.

Основными потенциально возможными каналами утечки информации являются:

- ✓ запоминание или копирование информации в процессе функционирования информационной системы;
- ✓ несанкционированное подключение к информационной системе;
- ✓ несанкционированный доступ к информации с помощью специальных устройств;
- ✓ изменение алгоритма работы системы;
- ✓ загрузка и использование сторонних программ вне общей технологии системы;
- ✓ проникновение сторонних программ - «вирусов»;
- ✓ использование незаконных технических средств (перехват электромагнитных волн и др.).

Существует множество разнообразных форм и методов контроля и защиты информации. Однако они должны работать синхронно и охватывать все элементы информационной системы. В связи с этим следует стремиться сочетать надежное аппаратное (техническое) и программное обеспечение с соответствующими организационными мерами.

При рассмотрении и анализе процессов контроля и защиты информации, очень трудно (а в большинстве случаев, невозможно) отличить функции контроля от

защиты. Если необходимо контролировать только функции управления, можно представить несколько типов элементов управления.

1. В зависимости от времени обращения виды контроля полностью соответствуют его основным формам и могут рассматриваться как **предварительный, текущий, последующий**.

При функционировании информационной системы под предварительным контролем понимается **контроль входной информации**, под текущим - **контроль при обработке** и под последующим - **контроль результирующей информации**.

- **Контроль входной информации (предварительный) -** выполняется перед выполнением каждой операции. Его основная цель - устранить предпосылки, которые могут привести к ошибкам. Выполняется по первичным документам, из которых вводится информация в технических средствах и по операциям ввода. Цель состоит в том, чтобы предотвратить ввод неверной информации в компьютер.
- **Контроль при обработке (текущий) -** осуществляется при выполнении операций. Здесь основную роль играет контроль, который встроен в программные продукты и функционирует непрерывно, взаимодействуя с основной программой. Текущий контроль развивается и проявляется параллельно с явлениями и процессами своего объекта, что раскрывает его оперативный характер, а предварительный контроль носит ярко выраженный превентивный (защитный) характер. Профилактика тоже находит место в текущем контроле, но с момента начала развития. Может найти применение в качестве «стопора» негативного развития и предотвращения накопления негативных эффектов. Функция «стопор» выполняет систему запретов и предупреждений, которая является неотъемлемой частью структуры любого современного программного продукта.
- **Контроль итоговой информации (последующий)** - целью этого контроля является устранение ошибок, допущенных к настоящему времени при обработке данных, и проверка вывода полученной информации. Для каждой технологической операции автоматизированной обработки данных применяются разные методы контроля.

Необходимо указать, что восприятие того или иного способа контроля зависит от типа используемых технических средств, технических носителей, типа и характера обрабатываемой информации, т.е. виды контроля используются в зависимости от конкретных условий и целесообразности.

2. В зависимости от технологии контроля, он может быть:

Автоматизированный (программное управление) - методы и средства управления являются неотъемлемой частью программного продукта. Он состоит из специальных операций, используемых при работе программного продукта. Эти операции устанавливаются программистами для управления действиями конечных пользователей Защита от случайных ошибок (непреднамеренное нажатие клавиши или сработавшая процедура). Наиболее важные из них являются:

- Инструкция по устранению ошибок;
- Вспомогательные тексты;
- Предупреждающие тексты;
- Инструкции по предыдущим и следующим операциям;
- Использование механизма альтернативного выбора;
- Использование механизма специально подготовленных номенклатурных полей;

- Контроль размера и формата данных;
- Контроль количества выполняемых операций;
- Контроль достижения заранее установленных лимитов.

Визуальный – пользователь осуществляет визуальный контроль над входной и выходной информацией, отслеживая работу программного продукта.

Каждая система защиты информации в корпорации должна одновременно отвечать некоторым общепринятым требованиям и иметь свои особенности.

Основные виды защиты информации являются следующие: спрятать, декомпозиция, дезинформация, разделение, страхование, отчетность, и шифрование.

Маскировка – это основной вид защиты, реализуемый на практике, и один из основных организационных принципов защиты информации. Максимально ограниченное количество пользователей, имеющих доступ к информационной системе, размещение и хранение информации в недоступных местах, а также ее секретность являются - основными средствами этого метода. Засекречивание информации на практике означает принадлежность к особой группе - секретная информация, с разной степенью секретности. В большинстве случаев она имеет различное значение для своего владельца и имеет к нему особый контролируемый доступ. Скрытая информация обычно исключает массовый доступ к информации, а также каналы ее утечки.

Декомпозиция – это вид защиты, который предполагает разделение секретной информации на степени секретности. Во время декомпозиции доступ к защищенной информации организуется, дифференцируется и регулируется. На практике это означает, что каждому отдельному пользователю предоставляются индивидуальные права на доступ к определенной информации, необходимой для выполнения определенных операций. Разграничение доступа может производиться на основе функциональных возможностей или на основе степени секретности информации. Декомпозиция как метод защиты информации является особым случаем сокрытия, потому что, если пользователю не разрешен доступ к информации, которая ему не нужна для выполнения своих официальных обязательств, это скрытая информация.

Дезинформация – это вид защиты информации, заключающийся в целенаправленном распространении заранее подготовленной ложной информации об истинном назначении отдельных объектов или продукции, фактическом состоянии организации или любой из сфер их деятельности.

Разделение - это вид защиты информации, который характеризуется тем, что разделяет защищаемую информацию на части с условием, что их очень сложно, а иногда и невозможно объединить, и добиться значимого результата.

Хранение новой информации – защищенная информация может использоваться повторно в течение неограниченного времени и большим количеством пользователей. Он обладает свойством не разрушаться и не терять своего объема, а в зависимости от использования может даже увеличиваться, т.е. для создания новой информации. Новая информация, в свою очередь, не имеет гарантии защиты и может создавать объективные предпосылки для уязвимости. Вновь созданная информация должна пройти обязательную проверку, прежде чем она будет сохранена и станет частью информационного ресурса организации.

Отчетность – это также один из важных методов защиты информации, обеспечивающий возможность в любой момент в процессе работы системы получать данные о состоянии защищаемой информации и ее пользователях.

Шифрование – это метод защиты информации, выражающийся в ее преобразовании с использованием различных кодов и алгоритмов. Шифрование использует набор символов и систему правил для преобразования информации в форму, недоступную для пользователей. Использование этой информации связано с обязательными операциями по ее декодированию. Шифрование информации может производиться как техническими, так и программными средствами.

Реализация этих основных типов защиты связана с разработкой комплекса организационных средств защиты информации, которые необходимо предоставить, чтобы повлиять на их реализацию. Наиболее важными из них являются:

- **наличие внутренней документации**, устанавливающей правила работы с компьютерным оборудованием и конфиденциальной информацией;
- **подписание дополнительных соглашений** к трудовым договорам сотрудников, в которых указана ответственность за разглашение или неправомерное использование секретной информации;
- **проведение инструктажей** и периодических проверок персонала;
- **разграничение сфер ответственности**, исключая, по возможности, ситуации, когда наиболее важные файлы данных доступны одному из сотрудников;
- **организация работы в общих программах,** которые в процессе своего функционирования осуществляют внутренний контроль;
- **организация хранения данных таким образом,** чтобы важные файлы не хранились вне сетевых устройств;
- **внедрение программных продуктов,** защищающих данные от копирования или уничтожения любым пользователем, включая высшее руководство организации;
- **составление планов восстановления системы** в случае отказа по любой причине.

Все эти комплексные меры должны входить в компетенцию ИТ-отдела компании и, в частности, службы безопасности. Если в компании нет такого отдела, можно пригласить внешнего специалиста по безопасности. Он может провести аудит ИТ-инфраструктуры компании и дать ценные советы о том, как защитить ее от внешних и внутренних угроз.

ВЫВОДЫ

В заключение можно сделать вывод, что для достижения надлежащего и полного контроля и защиты информации в корпоративной информационной системе, подход должен быть рассмотрен до ее создания и внедрения, а потом реализован последовательно. При организации информационной системы применяются как определенные базовые принципы, так и определенные организационные меры, направленные на создание необходимой среды, обеспечивающей безопасность корпоративных ресурсов.

Во-первых, необходимо интегрировать систему контроля и защиты информации. Целостность системы выражается в наличии единых целей ее функционирования, наличии информационных связей между элементами системы, иерархии ее отдельных функциональных единиц;

Во-вторых, система контроля и защиты информации должна обеспечивать безопасность информации и отстаивать интересы участников информационного процесса;

В-третьих, методы и средства, используемые системой управления информационной безопасностью, должны быть «прозрачными» для авторизованных пользователей. Желательно, чтобы они не создавали дополнительных неудобств, связанных с процедурами доступа к данным и их обработки;

В-четвертых, система контроля и защиты информации обязана обеспечивать информационные связи между элементами в ней, их совместное и согласованное функционирование, обеспечивать связи с внешней средой, в которой корпоративная информационная система представлена как единое целое;

В-пятых, необходимы упрощенные подходы к контролю и защите информации. Сложная система правил для полной безопасности столкнется с серьезными проблемами при ее реализации и нагрузкой на общение между сотрудниками. Правила контроля и защиты должны быть простыми в применении, а потребители, в свою очередь, должны осознавать их необходимость.

В-шестых, необходима четкая стратегия контроля и защиты. Сотрудники должны быть знакомы с четко определенными методами и средствами контроля и подчиняться им. Перед внедрением корпоративной информационной системы необходимо разработать правила работы для подготовки персонала. Программа контроля и защиты информации должна содержать все основные элементы, физические, программные и технические средства защиты, план работы с персоналом, план восстановления и т. д.

БИБЛИОГРАФИЯ

1. Галатенко П.К. Стандарты информационной безопасности, Москва, ИНТУИТ, 2006. 264 с. ISBN 5-9556-0053-1
2. Герасименко В. А. Защита информации в автоматизированных системах обработки данных, Енергоатомиздат, Москва 1994. 400с.
3. Мельников В. В. Защита информации в компьютерных системах. Финансы и статистика, Москва 1997. 368 с. ISBN 5-279-01631-4.
4. Шишманов К. Автоматизирани системи за контрол и защита на информацията. АИ Ценов, Свищов, 2008. 143 с. ISBN: 978-954-427-797-0
5. Highland H.J. Microcomputer security: Data protection techniques. Computers & Security, Volume 4, Issue 2, June 1985, Pages 123-134. ISSN: 0167-4048