ТЕХНИЧЕСКИЕ НАУКИ

Богданчиков Андрей Сергеевич
студент
ФГАОУ ВПО «Северо-Восточный федеральный
университет им. М.К. Аммосова»
г. Нерюнгри, Республика Саха (Якутия)
Герасимов Антон Михайлович
студент
ФГАОУ ВПО «Северо-Восточный федеральный
университет им. М.К. Аммосова»
г. Нерюнгри, Республика Саха (Якутия)
Гуримская Ирина Анатольевна
старший преподаватель
Технический институт (филиал)
ФГАОУ ВПО «Северо-Восточный федеральный
университет им. М.К. Аммосова»
г. Нерюнгри, Республика Саха (Якутия)

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Аннотация*: в статье рассмотрены наиболее частые угрозы информационной безопасности предприятия. Авторы указывают на способы их предотвращения.*

Ключевые слова*: угрозы, внешнее воздействие, внутреннее воздействие, вирусные атаки, несанкционированный доступ, резервирование.*

Суть информационной безопасности состоит в организации такого доступа к информации, который будет максимально защищен от любого реального и потенциального внешнего (или, возможно, внутреннего) воздействия на нее. Также

необходимо обезопасить движение информации между сотрудниками и клиентами в зависимости от типов производимых с ними операций. Для профилактики нежелательного удаления информации необходимо поддерживать возможность восстановления информации и её резервирования.

В зависимости от различных обстоятельств, таких как тип информации, используемой на предприятии, информационная безопасность может решать различные задачи. Среди них обеспечение качественного способа хранения информации, пресечение различных манипуляций с ней при передаче, организация надежного доступа к информации, мониторинг активности пользователей, многоступенчатая проверка с целью выявления и запрета несанкционированного доступа к информации, её резервирование и многое другое. Также установленный уровень безопасности необходимо поддерживать и совершенствовать в зависимости от возможных угроз.

1. Утрата и утечка информации

Среди причин потери информации выделяют две основные группы: внешнее и внутреннее воздействие.

Внешним является воздействие на информацию «со стороны», то есть посторонними лицами или организациями. Цели использования получаемой информации всегда разные: от личного интереса злоумышленника до нанесения вреда организации любыми возможными способами. Наиболее известным и используемым внешним воздействием является вирусная атака. Вирусные атаки могут повлечь за собой следующие опасности: удаления данных, их изменения, передачи злоумышленнику либо кому-либо еще, кто не имеет законного доступа к ней.

Внутреннее воздействие на информацию – воздействие через ПО, через сотрудников и устройства. Примером такого воздействия является халатность сотрудников, наличие легкий для взлома паролей, ненадежность которых может повлечь за собой взлом рабочего места и данных.

2. Способы защиты от угроз безопасности

Наиболее понятным любому пользователю способом защиты информации является наличие качественного и постоянно обновляемого антивирусного программного обеспечения. Использование лицензионных продуктов для работы почти полностью снижает риск наличия и запуска программных закладок, встроенных в рабочие программы и действующих не по прямому назначению. Также «пиратское» ПО негативно влияет на производительность ОС. В случае, если сотрудники часто покидают свое рабочее место, будь то по служебным делам или каким-либо еще, необходимо на время отсутствия блокировать доступ к их рабочему месту, чтобы защититься от использования рабочего места посторонними лицами. Так же уместно его пломбировать.

3. Типы негативных воздействий на информацию

Существует три группы негативных воздействий на информацию:

– разрушение оборудования, предназначенного для хранения информации. Причинами являются устаревание оборудования, некачественное производство, внешнее воздействие сотрудников (неосторожное обращение и т. п.);

– несанкционированный доступ. Злоумышленник, получив данные сотрудника предприятия, либо даже без них, может самостоятельно проводить операции с информацией, не имея на это права;

– вирусные программы, которые могут самостоятельно проводить операции с данными.

4. Программы, обеспечивающие защиту информации

Наиболее эффективным способом предотвращения воздействия на информацию является запуск защитных модулей как можно раньше при запуске операционной системы. Самым подходящим вариантом является защита загрузки системы с помощью пароля в BIOS и при загрузке операционной системы. Пароли следует не выбирать самостоятельно, а воспользоваться либо генераторами паролей, либо определителями мощности паролей. Подобное ПО можно найти в интернете в свободном доступе.

Права пользователей информацией должны быть предопределены в зависимости от занимаемой должности, уровня секретности информации, ее важности для производства и предприятия и по другим критериям. То же касается и работы по сети. Уязвимости системы и сети проверяются фаерволами и антивирусами. В случаях, когда информация может быть потеряна рекомендуется использовать утилиты для её резервирования и восстановления, если информация уже подверглась воздействию.

Список литературы

1. Безмалый В.Ф. Чем нас пытаются взломать (Краткий обзор программ-взломщиков паролей) / В.Ф. Безмалый, Е.В. Безмалая [Электронный ресурс]. – Режим доступа: www.citforum.ru

2. Редакция журнала 3DNews Сравнение сетевых сканеров безопасности, 2007 [Электронный ресурс]. – Режим доступа: http://www.3dnews.ru

3. Оглтри Т. Firewalls. Практическое применение межсетевых экранов, ДМК Пресс, 2003 [Электронный ресурс]

4. Астахов А. Разработка эффективных политик информационной безопасности // IT Директор. – 2005. – Январь.

5. Филиппов М.В. Проблемы защиты и резервирования информации в современных информационных системах, 2006 [Электронный ресурс]. – Режим доступа: http://www.kacha.ru