ЗНАЧЕНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ БИЗНЕСЕ

Калинин Денис Дмитриевич

Московский технологический университет (119454, г. Москва, Проспект Вернадского, д.78) e-mail:rector@mirea.ru

В постиндустриальной экономике произошло бурное развитие средств автоматизированной обработки информации (АСОИ). Это послужило причиной для формирования целого ряда проблем, связанных с обеспечением информационной безопасности по всем направлениям человеческой жизнедеятельности: в политике, бизнесе, социальных вопросах, культуре, международной деятельности и пр.

Под термином «информационная безопасность» (ИБ) применительно к коммерческому предприятию принято понимать защищенность от возникающих угроз внешнего и внутреннего характера, которые возникают в процессе хозяйственной деятельности[2]. Они угрожают информации и нематериальным ценностям компании, подрывая основы ее конкурентоспособности и нарушая нормальный порядок функционирования в рыночной среде.

В структуру системы обеспечения безопасности предприятия входят основные элементы, правильно выстроенное взаимодействие которых обеспечивает ее работу[1].

Элементы системы обеспечения информационной безопасности:

- любой информационный объект защиты (содержательная часть или процесс) имеет своего владельца, которые отвечает не только за состояние, актуальность и содержание ресурса, но и за его безопасность;

- для любой информации существует окружающая среда (внешняя и внутренняя), которая является источником потенциальной или реализованной угрозы;

- анализ существующих угроз и рисков, которые воздействуют на очевидные или скрытые уязвимости, присутствующие в данной информационной системе;

- перечень мероприятий, направленных на обеспечение информационной защиты;

- наконец, сами информационные ресурсы (содержательные и процессные), которые являются объектом информационной защиты.

Ключевые слова: Бизнес, информационная безопасность

THE IMPORTANCE OF THE INFORMATION SECURITY SYSTEM IN MODERN BUSINESS

Kalinin Denis Dmitrievich

Moscow University of Technology (119454, Moscow, Vernadsky Prospekt d.78) e-mail: rector@mirea.ru

In the post-industrial economy there was a rapid development of the means of automated information processing (ASOI). This was the reason for forming a number of problems related to ensuring information security in all areas of human life: in politics, business, social issues, culture, international activities, etc.

Under the term "information security" (IB) with respect to a commercial enterprise, it is customary to understand the protection from emerging threats of external and internal nature that arise in the course of economic activityx[2]. They threaten information and intangible values of the company, undermining the basis of its competitiveness and disrupting the normal order of functioning in a market environment.

The structure of the enterprise security system includes the basic elements, the properly structured interaction of which ensures its operation[1].

Elements of the information security system:

- any information protection object (content part or process) has its owner, which is responsible not only for the state, relevance and content of the resource, but also for its security;

- for any information there is an environment (external and internal), which is the source of a potential or realized threat;

- An analysis of existing threats and risks that affect the obvious or hidden vulnerabilities present in this information system;

- a list of activities aimed at ensuring information protection;

- Finally, the information resources themselves (content and process), which are the object of information protection.

The Key Words: Business, information security

В постиндустриальной экономике произошло бурное развитие средств автоматизированной обработки информации (АСОИ). Это послужило причиной для формирования целого ряда проблем, связанных с обеспечением информационной безопасности по всем направлениям человеческой жизнедеятельности: в политике, бизнесе, социальных вопросах, культуре, международной деятельности и пр.

Под термином «информационная безопасность» (ИБ) применительно к коммерческому предприятию принято понимать защищенность от возникающих угроз внешнего и внутреннего характера, которые возникают в процессе хозяйственной деятельности. Они угрожают информации и нематериальным ценностям компании, подрывая основы ее конкурентоспособности и нарушая нормальный порядок функционирования в рыночной среде.

В структуру системы обеспечения безопасности предприятия входят основные элементы, правильно выстроенное взаимодействие которых обеспечивает ее работу (рис.1).

Рисунок 1 – Взаимосвязь структурных элементов системы обеспечения информационной безопасности предприятия

Элементы системы обеспечения информационной безопасности:

- любой информационный объект защиты (содержательная часть или процесс) имеет своего владельца, которые отвечает не только за состояние, актуальность и содержание ресурса, но и за его безопасность;

- для любой информации существует окружающая среда (внешняя и внутренняя), которая является источником потенциальной или реализованной угрозы;

- анализ существующих угроз и рисков, которые воздействуют на очевидные или скрытые уязвимости, присутствующие в данной информационной системе;

- перечень мероприятий, направленных на обеспечение информационной защиты;

- наконец, сами информационные ресурсы (содержательные и процессные), которые являются объектом информационной защиты.

Следует различать понятия «безопасности» и «отсутствие опасности», поскольку достаточно часто происходит их подмена и, как следствие, возникает путаница при определении ключевых терминов и понятий. «Не опасен» с точки зрения деятельности коммерческой компании такой негативный фактор, который в данных условиях или при их изменении не повлечет за собой изменение любых характеристик данного предприятия. К примеру, для деятельности промышленной корпорации не является опасным негативный фактор утечки в открытый доступ расписания движения вахтового автобуса, доставляющего персонал к удаленному месту работы. В то же время попавшая к конкурентам уникальная технология приготовления строительной смеси может нанести серьезный ущерб на стратегической перспективе, подорвав основы коммерческой деятельности[3].

Безопасным же фактором для компании, даже если он имеет негативные характеристики, будет являться тот фактор, который способен отрицательно повлиять на стабильность деятельности (или состояния) данного предприятия, однако при этом не может реализовать собственный негативный потенциал, поскольку учреждение способно оказывать внутреннее сопротивление подобному воздействию и успешно реализует эту свою способность. Например, серьезные репутационные риски могли бы последовать за утратой информации о клиентской базе предприятия; однако предусмотрены резервное копирование, разграничение прав доступа к информационным данным, используются авторизация пользователей и другие методы защиты, что снижает данный риск до минимума.

При этом следует понимать, что только комплексный подход к обеспечению информационной безопасности в состоянии гарантировать стабильную и бесперебойную работу предприятия при любых внешних и внутренних угрозах (рис. 2).

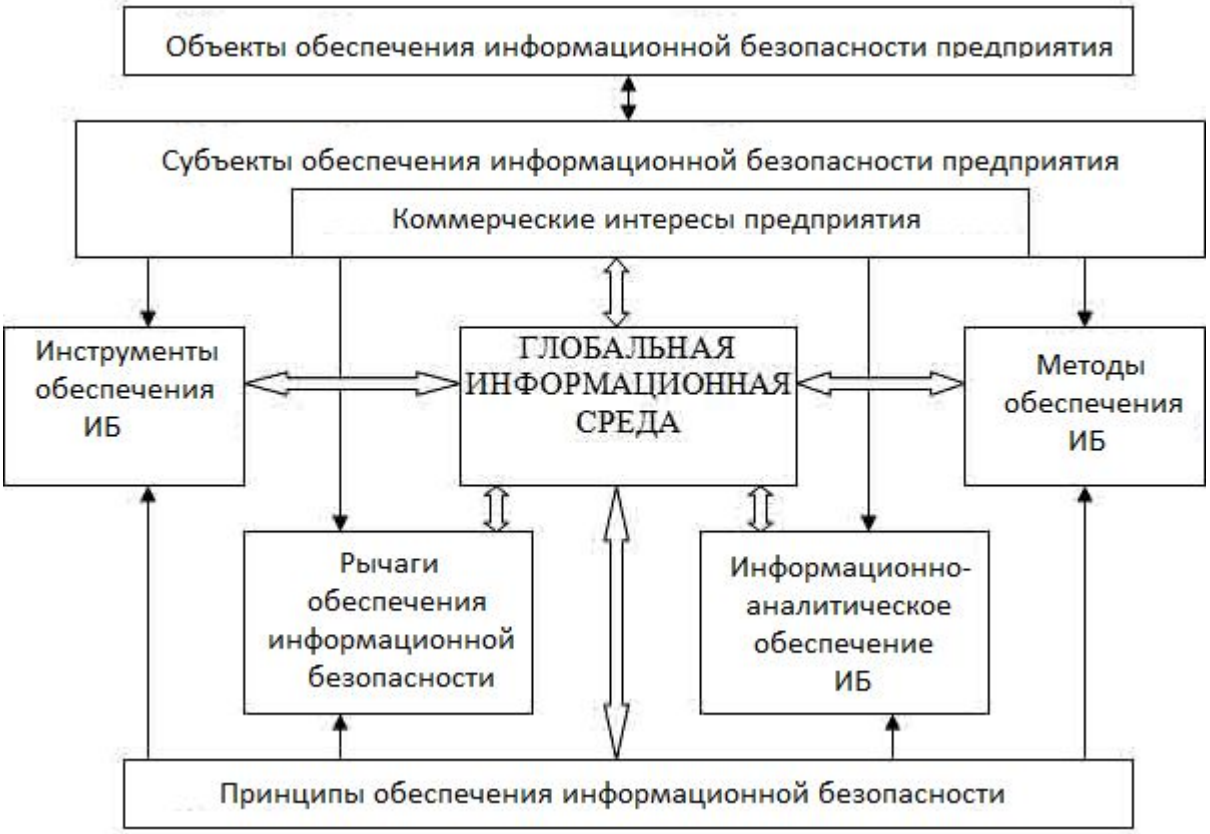

Рисунок 2 – Комплексный подход к формированию системы обеспечения информационной безопасности предприятия

С точки зрения управления информационной безопасностью учреждения, крайне важно понимать принципы функционирования обратной связи – то есть своевременного получения точных данных о текущем состоянии объекта защиты, оценки и анализа данной информации. Сущность оценки информационной безопасности компании состоит в выборе соответствующих критериев и показателей, позволяющих получить в оперативном порядке объективные данные о ключевых процессах жизнедеятельности данного предприятия[5].

Критерии и показатели должны быть установлены для каждого направления информационной защиты безопасности отдельно.

К примеру, для информационной безопасности учреждения необходимо учитывать следующие базовые оценочные критерии:

1. Конфиденциальность, то есть соответствие утвержденного и фактического перечня людей, имеющих служебный доступ к коммерческой информации, тем задачам, которые они решают в процессе выполнения своих непосредственных служебных обязанностей. Показателями, которые определяют, соблюдается ли требование конфиденциальности, являются:

- минимальное и достаточное число имеющих доступ к информации лиц;

- продуманный порядок получения доступа к информации различного уровня, что исключает случайное приобретение прав манипуляции с коммерческими данными;

- применение современных средств и методов технической, цифровой, психологической, организационной защиты информации, и др.

Для России вопрос сохранения конфиденциальности остается пока самым проработанным аспектом системы обеспечения ИБ как с точки зрения законодательной базы, так и в аспекте технических средств и методов защиты, перекрывающих все возможные каналы, допускающие возможность информационной утечки[4].

2. Целостность информации, то есть обеспечение того, что информация поступит пользователю в полном и неискаженном виде. Достаточно часто бывает, что утеря части информации приводит к более серьезным негативным последствиям, чем полная утеря информации – хотя бы потому, что полная утеря данных является очевидной, в то время как искажение или частичное отсутствие информации может оказаться не сразу замеченным пользователем.

Целостность бывает статической (когда информационные объекты остаются в неизменном состоянии) и динамической (когда сложные информационные процессы протекают штатно, корректно и без сбоев). На данном этапе статическая целостность имеет более серьезное подкрепление, чем динамическая. При этом следует отметить, что защита динамических информационных потоков является крайне значимой – работа в этом направлении позволяет вовремя пресечь или выявить попытки уничтожения, изменения или копирования информационных объектов защиты.

3. Доступность информации подразумевает возможность пользователю, имеющему соответствующий доступ, получать нужные ему сведения своевременно и эффективно (то есть при соизмеримых значимости информации усилиях). Если происходит сбой по срокам получения информации, либо получение простейших сведений требует значительных трудозатрат, то система начинает тормозить деятельность всех функциональных подразделений, то есть становится неэффективной и наносит ущерб коммерческой деятельности предприятия. Данный факт также подтверждает значение доступности как критерии оценки эффективности работы системы обеспечения информационной безопасности.

Таким образом, информационная безопасность компании по сути означает ее способность успешно противостоять постоянно возникающим негативным информационным факторам внешнего и внутреннего характера, угрожающим стабильности и нормальной жизнедеятельности учреждения. Для каждого из направлений, по которым информационной безопасности учреждения может угрожать какое-то негативное воздействие, следует разработать собственную систему оценочных критериев и показателей, которые способны дать своевременную, точную, непротиворечивую и объективную информацию о текущем состоянии информационной безопасности учреждения.

Список литературы

1. Р., М. Алгулиев Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных сетей / Р. М. Алгулиев. - М.: УРСС, 2001. - 248 с.

2. Андрианов, В. В. Обеспечение информационной безопасности бизнеса / В.В. Андрианов. - Москва: Мир, 2010. - 627 с.

3. Андрианов, В.В. Обеспечение информационной безопасности бизнеса / В.В. Андрианов. - М.: Альпина Паблишер, 2011. - 871 с.

4. Варлатая, С. К. Криптографические методы и средства обеспечения информационной безопасности. Учебное пособие / С.К. Варлатая, М.В. Шаханова. - М.: Проспект, 2015. - 152 с.

5. Горев, А И; Симаков А А Обеспечение Информационной Безопасности / А Горев А И; Симаков А. - Москва: Гостехиздат, 2005. - 474 с.