**УДК**

**004.056**

**Особенности управление информационной безопасностью кредитно-финансовых структур региона**

**Special features control of information security credit and financial intuitions region**

**Соляной В.Н., СухотеринА.И., Сиротский А.А. , Морозов О.В.** Финансово-технологическая академия, г. Королев, Россия

**Solyanoy V.N., Sukhoterin A.I., Sirotski A.A.,** **Morozov O.V**. Financial and Technological Academy, Korolev city, Russia

Аннотация. Базовые принципы построения эффективной системы управления информационной безопасностью кредитно-финансовой организации.

С чего начать построение процессов информационной безопасности? Как организовать взаимодействие между подразделениями? Как определять эффективность? Об этом и многом другом – в статье о построении службы информационной безопасности банка.

Annotation. Basic principles of creation of an effective control system of information security of the credit and financial organization.

From what start construct information security process? How organize interaction between organization parts? How determine the effectiveness?

About this and many another question’s in publication of the bank information security building

Ключевые слова. Информационная безопасность кредитно-финансово структур, защита информация, планирование, реализация стратегия.

Key words: information security of credit and financial intuitions region, information defense, planning, realization strategy.

**Описание проблемы**

Несмотря на имеющиеся нормативные требования по наличию выделенной структуры по информационной безопасности в кредитно-финансовых учреждениях, многие банки до сих пор озадачены этим вопросом

Как правило, функции ИБ сконцентрированы в службе ИТ. Из практики, Службу ИБ выделяют либо из существующей службы ИТ, либо создают «с нуля». В первую очередь перед менеджером по информационной безопасности встают проблемы не только соответствия требованиям нормативной документации и регуляторов, но и требованиям бизнеса

Для этого как минимум необходимо выстроить процессы ИБ между службой ИБ и другими службами в банке. На рис. 1 приведен перечень служб, которые, как правило, существуют в любой кредитно-финансовой организации. Мы ответим, как минимум на следующие вопросы:

* Какие службы привлечь?
* Как организовать взаимодействие?
* Какие процессы внедрить?
* Как обеспечить отчетность?
* Как отслеживать эффективность
* Как следить за изменения в бизнесе?
* Как удостовериться, что остаточный риск- приемлем?
* Как организовать контроль и выполнимость требований ИБ?



**Рисунок 1 - Перечень служб, участвующих в процессе организации менеджмента ИБ**

Планирование работы

В первую очередь, менеджеру по информационной безопасности необходимо определить, какие требования я применимы, оценить текущую степень соответствия. Для этого проводится самооценка соответствия обязательным требованиям регуляторов и нормативной документации. Также менеджер по ИБ получает требования по защите активов от владельцев бизнес процессов.

Далее, определив применимые требования и точки несоответствия, необходимо провести презентацию результатов руководству банка. Непосредственно результаты этого этапа будут являться «точкой отсчета» для измерения результативности работы службы информационной безопасности. На этом этапе менеджер по ИБ должен убедить руководство в необходимости реализации тех или иных требования, связав их с генерирующими прибыль процессами банка.

С позиции руководства не важно, какие требования менеджер предлагает реализовать и для чего. Руководству важно понять выгоду для бизнеса от реализации этих требований и риски, которые возникают в случае их не реализации. Это касается как требований к защите активов, так и требований регулирующих органов. Любые требования следует трактовать с позиции риск-менеджмента.

Несоответствие требованиям регуляторов может привести к санкциям с их стороны, денежным штрафом, отзывом лицензии на осуществление основного вида деятельности. Отказ в защите бизнес-активов может привести к потере доверия клиентов, партнёров, контрагентов. Все эти риски должны быть учтены, связаны с основным бизнесом банка и доведены до руководства.

В конечном итоге руководство решает, является ли указанный риск приемлемым. Зачастую то, что может быть критично с точки зрения структурных подразделений (владельцев бизнес-процессов), менеджера по информационной безопасности, руководством может быть отнесено на второй план. Связав риски либо их совокупность с генерирующей прибыль деятельностью можно дать понять руководству реальную степень угрозы.

**Рисунок 2 - Организация планирования ИБ кредитно-финансовых структур региона**

Заручившись поддержкой руководства в реализации процессов управления информационной безопасностью, менеджеру по ИБ необходимо приступить к непосредственной их реализации. С практической точки зрения это означает выпуск приказа по банку с указанием ответственных за разработку процессов (как правило, это менеджер по ИБ), вовлекаемых подразделений, их ответственность в рамках работы менеджера по ИБ и контроля исполнения.

Ознакомление с приказом и доведение его до всех подразделений важно – поскольку это демонстрирует вовлеченность руководства банка и является мотивирующим фактором для задействованных подразделений. Необходимо, чтобы все сотрудники ощутили, что инициатива исходит не от одного конкретного человека, сотрудника «какой-то» службы ИБ, а от руководства банка в качестве одного из процессов управления.

**Реализация стратегии**

Перед началом реализации процессов менеджеру по ИБ необходимо разработать стратегию информационной безопасности. При разработке стратегии необходимо обязательно учесть требования бизнеса, а также некоторый период его развития.

****

**Рисунок 3 - Реализация стратегии ИБ кредитно-финансовых структур региона**

На основании стратегии разрабатывается политика ИБ, которая содержит требования ко всем применяемым технологиям, системам и подсистемам. Однако такой документ не следует перезагружать специфической терминологией: он должен описывать требования в понятной и доступной форме и детализироваться, при необходимости, отдельными документами с учетом и области распространения.

На **рис. 3** представлены процессы, которые могут быть в той или иной степени делегированы различным структурным подразделениям банка. На рисунке изображен лишь тот необходимый минимум, который возможно эффективно интегрировать.

**Совершенствование**

После разработки и реализации в банке процессов информационной безопасности важным фактором успешного их функционирования является применение классического цикла PDCA.

Мониторинг и совершенствование являются хорошим подходом, однако на практике это вызывает сложности, которые связаны с входной и выходной информацией этих процессов. Как правило, руководства банка и менеджер по ИБ проводят недостаточно встреч, либо не проводят их совсем. Связанно это в первую очередь с тем, что руководство не хочет получать избыточную информацию, которой изобилуют отчеты службы ИБ.

На **рис. 4** представлен план внутреннего взаимодействия, оптимально представляющего различные метрики эффективности в рамках вовлеченных в управление ИБ структурных подразделений.

**Рисунок 4 - Совершенствование менеджмента ИБ кредитно-финансовых структур региона**

**Вывод**

Информационная безопасность – важный процесс в управлении любой организацией и должен являться неотъемлемой частью общего менеджмента организации. Мы рассмотрели каким образом его можно встроить в существующие процессы банка, тем самым повысив эффективность и результативность деятельности службы ИБ.

Ни в коем случае нельзя допустить, чтобы служба ИБ существовала отдельно. При такой работе требования бизнеса не будут учтены, руководство не будет осведомлено о целях и задачах ИБ, что непременно повлечет урезание бюджета и сведет результативность ИБ к минимуму.

**Используемая литература**

1. Распоряжение Правительства РФ от 03.11.2011 № 1944-р   
   «О перечне направлений подготовки (специальностей) в образовательных учреждениях высшего профессионального образования, специальностей научных работников, соответствующих приоритетным направлениям модернизации и технологического развития российской экономики» Официальная публикация в СМИ: "Российская газета", № 254, 11.11.2011 "Собрание законодательства РФ", 14.11.2011, № 46, ст. 6584
2. Материалы пленума учебно-методического объединения вузов Российской Федерации по образованию в области историко - архивоведения. РГГУ «Институт информационных наук и технологий безопасности». Сборник аннотаций программ учебных дисциплин ОООВПО по направлению подготовки 090900 «Информационная безопасность» квалификация: бакалавр. Профили: «организация и технология защиты информации», «Комплексная защита объектов информации». – М. 2012г.
3. ООП ВПО 090900.62 Информационная безопасность, квалификация (степень) выпускника «Бакалавр», форма обучения – очная, нормативный срок освоения программы - 4 года. Утверждена УМС ФТА: Протокол №01 от «24» сентября 2013 г.
4. Методические материалы по обучающему комплексу по направлению подготовки 090900 информационная безопасность квалификация (степень) бакалавр и магистр: Санкт- Петербург 2013 г.
5. Соляной В.Н., Сухотерин А.И.. Обоснование открытия на ОАО ТРВ базовой кафедры по обеспечению комплексной безопасности предприятий. г. Королев. Сборник научных трудов, Информационно-технологического факультета. ФТА. 2012г.
6. Соляной В.Н., Сухотерин А.И.. Взаимодействие человека, техники и природы: проблема информационной безопасности. Научный журнал (КИУЭС) Вопросы региональной экономики. УДК 007.51 №5 (05) г. Королев. ФТА. 2010г.

Сухотерин А.И., Соляной В.Н. Взаимодействие человека, техники и природы: проблема информационной безопасности. Вопросы региональной экономики. – Королев.: Т.5.№5., 2010, 86-91 с.

1. Федоров М.А. Соляной В.Н. Теоретические основы методик выявления и прогнозирования электромагнитных угроз безопасности функционирования управления космическими системами. В сборнике: [Сборник научных докладов Международной научно-практической конференции, посвященной празднованию 150-летия со дня рождения В.И. Вернадского](http://elibrary.ru/item.asp?id=20483157) руководитель проекта Старцева Т.Е.. 2013. С. 210-214.
2. Тарасов А.И., Федоров М.А. Анализ проблемы обеспечения энергоинформационной безопасности типового предприятия и пути ее разрешения. Наука - промышленности и сервису: Сб. стат. 6 международной научно-практической конференции. Ч.П/ Поволжский гос. ун-т сервиса.- Тольятти: Изд-во ПВГУС, 2012, №6-2. 372-380 с.