ВТБ Капитал

Информационная безопасность в финансовом секторе, есть ли повод к управленческим решениям

Апрель 2016

Андрей Бажин
Директор по информационное безопасности
ВТБ Капитал

Содержание

- Причины структурных перемен и фундаментальные требования к ИТ и ИБ
- Обзор присущих рисков для финансового сектора
- Факторы влияющие на выбор модели управления ИБ
- Место ИБ в новой структуре
- Роль мотивации и «мягких» методов управления
- Методологический базис для изменений ИБ
- Обзор новых-старых технологий ИБ

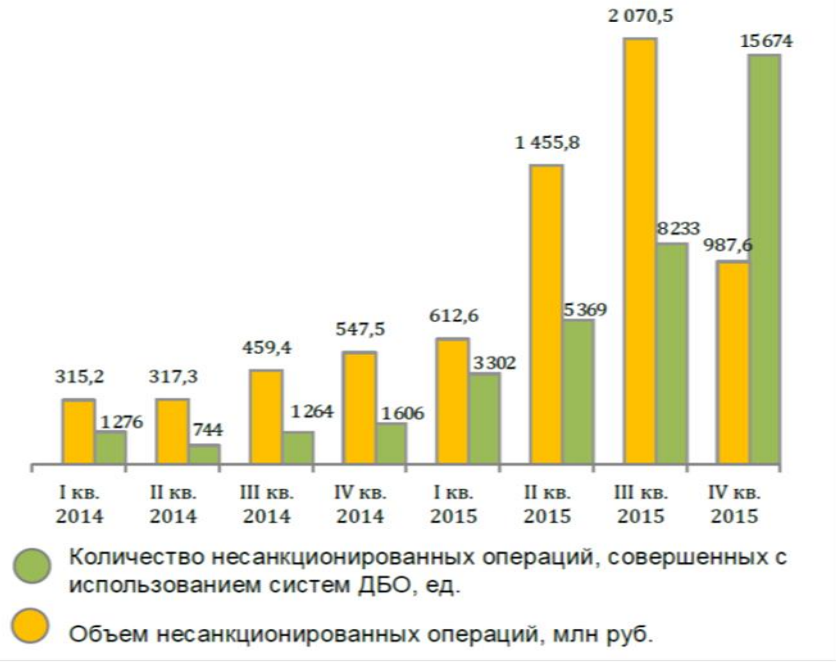
Причины структурных перемен и фундаментальные требования бизнеса к ИТ и ИБ

Ключевые Факторы	Стратегические задачи
Тренд регулятора ЦБ РФ, отраженный на Уральском форуме – продолжить развитие СТОБР, 382-П и гармонизировать работу по защите ПДн с Роскомнадзором, ФСТЭК и ФСБ	Переход от Компьютерной безопасности к стратегической программе обеспечения ИБ для всех критичных бизнес процессов в финансовой организации. Определение целевого уровня ИБ на 2-3 года
Смещение фокуса атак на финансовые организации	Оптимизация системы контролей в том числе в части редизайна операционной деятельности. Установка системы KRI для данного риска. Постоянное управление риском. Работа через ассоциации и ЦБ РФ с МВД и Думой по примеру работы, которая была проведена с фродом в части пластиковых карт
Изменение курса рубля, так называемая – «новая реальность»	Повышение эффективности, результативности ИБ, приближенность к операционным рискам и коллегиальным органам управления
Серьезные изменения в финансовом секторе, как в части сокращения игроков, так и смене ИТ платформ и появления новых технологий	Для тех Финансовых организаций, где ИБ не было – создание выделенных подразделений, так где ИБ есть - вывод ИБ из ИТ или разделение ИБ и Компьютерной безопасности

Обзор присущих рисков для финансового сектора

- Основным риском, который имеет прямые финансовые последствия остается **риск мошенничества**
- Риск влияет, как на клиентов подрывая доверие к дистанционным средствам обслуживания, так и на сами финансовые организации, которые стали нести прямые потери от атак на АРМ КБР
- Плюс - Риск стать стоп фактором в развитии бизнеса и/или ИТ

Динамика количества и объема несанкционированных операций, совершенных с использованием систем ДБО



* http://cbr.ru/PSystem/P-sys/survey_2015.pdf

Несанкционированный доступ в платежную систему

- По версии Энергобанка, 27.02. 2015г. с 12:30 до 12:43 некие злоумышленники получили контроль над терминалом банка и провели на Московской бирже ряд несанкционированных операций по покупке и продаже валюты. По таким неудачным курсам, что в результате этих операций банк, как уверяют представители брокерских компаний, потерял около 370 млн. рублей

Прочие критичные случаи

- Полтора десятка банков-участников Объединенной расчетной системы стали жертвами масштабного мошенничества с платежными картами. Инцидент, имел место 16/08/2015 года, под ударом оказалось ~ 500 миллионов рублей
- Взлом перед новым 2016 годом АРМов отправки платежей в нескольких банках РФ, каждый банк потерял порядка USD 10 млн
- 2016 февраль: Металлинвестбанк – попытка хищения, атака на АРМ КБР, возможные потери ~200 миллионов

http://ria.ru/incidents/20160305/1385351434.html

Плюс криптолокеры

Точечные атаки на финансовые организации

В ходе совместного расследования «Лаборатория Касперского», Европол и Интерпол раскрыли беспрецедентную киберпреступную операцию, в рамках которой злоумышленники похитили миллиард долларов США. Киберограбление продолжалось два года и затронуло около 100 финансовых организаций по всему миру. Эксперты полагают, что за этим громким инцидентом стоит международная группировка киберпреступников из России, Украины, ряда других европейских стран, а также Китая

Как происходила атака :

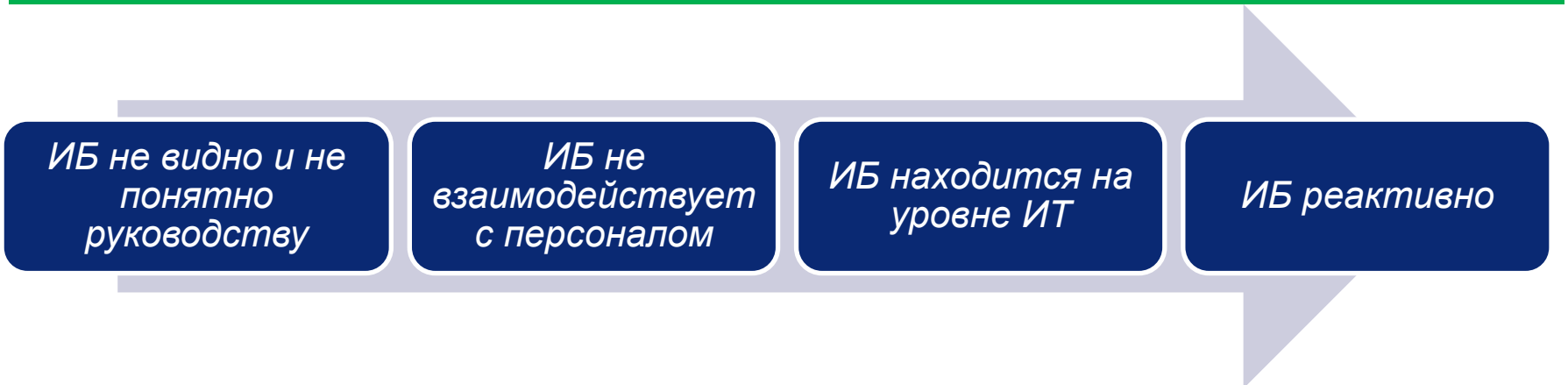
1. В среднем ограбление одного банка — от заражения первого компьютера в корпоративной сети до кражи денег и сокрытия следов — занимало у хакеров от двух до четырех месяцев
2. Средняя сумма кражи ~10 000 000 USD
3. Заражение проходило или через **письмо с вложением**, как бы от сотрудника банка или клиента или через фишинг – по **ссылке** на WWW ресурс в который предлагалось ввести логин и пароль; сотрудники вводили свои логин и пароль в подложный сайт имитировавший корпоративный ресурс или систему
4. Далее злоумышленники собирали информацию о процессе работы банка и находили удобный момент для совершения кражи, в том числе использовали для вывода средств S.W.I.F.T (который на первый взгляд кажется абсолютно защищенным) или системы дистанционного банковского обслуживания
5. Искажали балансы, что бы сумма списания не была видна сразу

Модель мошенничества

Влиять на мотив и наказание мошенника можно только опосредованно и реактивно, а снижать вероятность можно всегда, если создавать безопасную экосистему!

Что привело к реализации указанных рисков

Типичный вариант ответа – не дали денег на ИБ, но если подумать, то:



Т.е. на мой экспертный взгляд, в первую очередь играет не недостаток средств, а следующие факторы:

- Недостаточное внимание менеджмента, отвечающего за операционный блок, с одной стороны, и не готовность ИБ и куратору ИБ поставить вопрос ребром
- Недостаточная работа ИБ с персоналом
- Отсутствие реальной ИБ, когда вместо управляемой системы контролей есть набор средств защиты

Т.е. прежде всего были сделаны ошибки на уровне управления

Факторы влияния на выбора модели управления ИБ

Нет одинаковых рецептов, но есть ориентиры

- *Уровень зрелости ИТ*, если в ИТ хаос, то в ИБ будет его отражение, но если в ИТ внедрен ITIL, то и ИБ должна быть встроена в сервисную модель
- *Уровень зрелости управления операционным риском*, если есть предпосылки по сквозному управлению ОР, то управление рисками ИБ должно быть интегрировано в общую систему управления рисками, как минимум в части KRI, базы инцидентов, если есть GRC и т.д.
- *Зрелость коллегиальных органов управления,* как минимум участие в ИТ комитете в качестве полноценного члена с правом голоса
- *Отсутствие процессов ИБ*, замкнутость на средства защиты – важный критерий необходимости выделения ИБ из ИТ или ВБ
- *Наличие посредника между ИБ и членом правления курирующим ИБ*
- *Отсутствие ИБ, как выделенного подразделения* – явный критерий, как минимум, выделить одного специалиста

«Работа работой, но надо и что-то полезное делать. Хенрик Ягодзиньский.

Место ИБ целевой структуре

Лучше развивать ИБ эволюционно интегрируясь в бизнес и контрольную среду

Методологический базис для изменений ИБ

Регуляторная активность вышла на хороший продуктивный уровень и ЦБ и ФСТЭК и ФСБ и Роскомнадзор активно выпускают нормативы. Информация по большей части разрабатываемых документов была озвучена на Уральском форуме

Но есть проблема:

- На текущий момент, на мой взгляд, основным камнем преткновения является, то что регуляторы разрабатывают документы на техническом языке для технических специалистов
- Есть недостаток качественных трансляционных материалов по регуляторной теме, которую стоило бы доводить до руководства финансовых организаций от регуляторов. Т.е. функция «толмача» законов отводиться не регуляторам, а интеграторам, которые предлагают соответствие за деньги или техническим специалистам. И часто перегибают палку пытаясь раздуть требования до нужных им объемов
- По этой причине все обозначенные на Уральском форуме инициативы по выходу новых документов, могут буксовать в части претворения в жизнь, т.к. а) голос ИБ внутри организаций слаб б) в стране новая реальность и надо экономить с) интеграторы не всегда на стороне потребителей и руководство видит, что риск не сопоставим с затратами, что взывает недоверие и тормозит процесс

Обзор новых-старых технологий ИБ

Новое хорошо забытое старое:

- ИТ полным ходом идет в сторону сервисной модели в том числе облачных сервисов
- На волне рисков фрода заиграли сервисы Threat intelligence и системы обнаружения атак внутри сети и песочницы; Заработал финсерт ЦБ РФ
- Появляются российские сервисы аутсорсинга ИБ; в том чсле SOC и важно не просто получить лог, но реально уметь найти в логе подозрительные следы
- Все больше и больше становится вытребована бизнесом мобильность – BYOD, удаленный доступ и т.д., т.е. нужно заранее выбирать платформу для MDM, 2FA, готовить юридическую базу
- В свете укрупнения банков возможны проекты по смене АБС
- Розница переходит с ПК и windows на смартфоны, т.е. IOS и андройд
- Поднимаются вопросы о контроле кода SDLC

Выводы

1. До начала инфраструктурных изменений у ИБ должна быть компетенция в части указанных выше областей развития ИТ,
2. У ИБ должна быть более ярко выраженная специализация, универсалом практически невозможно остаться, надо делать выбор в каком направлении развиваться,
3. Сейчас хорошее время провести анализ рисков и дать предложения о целевом уровне ИБ на 2 -3 года.

Об авторе

Андрей Бажин
Директор по информационной безопасности
ВТБ Капитал

www.vtbcapital.com

Настоящий документ подготовлен АО ВТБ Капитал (далее – «ВТБ Капитал»), носит исключительно информационный характер и предназначен только для лиц, являющихся допустимыми получателями.

Настоящий документ не является проспектом ценных бумаг, обязательством по размещению ценных бумаг, предложением по финансированию, офертой или приглашением делать оферты на покупку или продажу каких-либо ценных бумаг или иных финансовых инструментов. При оценке любых инвестиционных продуктов или стратегий, вы должны самостоятельно (с привлечением собственных налоговых, бухгалтерских, финансовых и/или юридических консультантов) определить приемлемость любых финансовых инструментов или сделок до принятия инвестиционного решения. Настоящий документ (или какая-либо его часть) не является налоговым, юридическим, бухгалтерским, финансовым или инвестиционным советом и не должен интерпретироваться как таковой. Несмотря на всю тщательность подготовки настоящего документа, никто из руководителей, менеджеров, сотрудников, агентов или консультантов любой компании Группы ВТБ не дает каких-либо гарантий или заверений, выраженных или подразумеваемых, и не принимает на себя какой-либо ответственности в отношении надежности, точности или полноты информации, содержащейся в настоящем документе.

«ВТБ Капитал» не принимает на себя какой-либо ответственности за любые убытки (прямые или косвенные, предвиденные и непредвиденные), возникающие в связи с использованием настоящего документа или содержащейся в нем информации. «ВТБ Капитал» не берет на себя обязательств по обновлению информации в настоящем документе. Вся информация, мнения и оценки даны по состоянию на дату публикации настоящего документа и могут быть изменены без предварительного уведомления. Информация в настоящем документе не предназначена для предсказания фактических результатов, и «ВТБ Капитал» не дает каких-либо гарантий и заверений в этом отношении.

Стоимость любых инвестиций может увеличиваться и уменьшаться в результате изменений на рынке. Результаты инвестирования в прошлом не гарантируют доходов в будущем.

Определенные сделки, в том числе с фьючерсными контрактами, опционами и прочими производными инструментами связаны с повышенной степенью риска и не могут быть одинаково приемлемы для всех инвесторов. Ряд лиц – как физических, так и юридических – может быть ограничен в праве совершения сделок на рынках ценных бумаг. Инвесторам следует проводить собственную юридическую экспертизу до принятия инвестиционного решения. Важно отметить, что ценные бумаги и финансовые инструменты, деноминированные в иностранной валюте, американские депозитарные расписки и прочие инвестиционные инструменты зависят от валютных курсов, колебания которых могут негативно отразиться на стоимости инвестиций. Стоимость инвестиций может как увеличиваться, так и уменьшаться, поэтому инвесторам не может быть гарантировано возвращение инвестированных средств в полном объеме.

Группа ВТБ может находиться в деловых отношениях или стремиться к установлению таковых с компаниями, упомянутыми в настоящем документе. Инвесторы должны осознавать возможность конфликта интересов, который может повлиять на объективность настоящего документа, поскольку компании Группы ВТБ и/или их собственники, руководители, менеджеры и сотрудники (включая, кроме прочих, лиц, участвовавших в подготовке и публикации настоящего документа) могут владеть ценными бумагами или финансовыми инструментами, упоминаемыми в настоящем документе, иметь по ним открытые позиции или совершать с ними сделки; могут осуществлять инвестиции в отношении любого из упоминаемых в настоящем документе эмитентов; могут участвовать в операциях с ценными бумагами в форме, не согласующейся с информацией в настоящем документе в отношении ценных бумаг или финансовых инструментов, упомянутых в настоящем документе; могут продавать их клиентам или покупать их у клиентов, выступая в роли принципала; действовать в качестве руководителя, агента по размещению, консультанта или кредитора; проводить маркетинговые мероприятия; выступать в качестве организатора или соорганизатора последнего по времени публичного размещения в отношении любых инвестиций или эмитентов таких ценных бумаг или финансовых инструментов, упомянутых в настоящем документе; предоставлять или предлагать инвестиционно-банковские или иные услуги любой из компаний, упомянутых в настоящем документе.

Деятельность АО ВТБ Капитал в Российской Федерации лицензируется и регулируется Центральным Банком России. VTB Capital plc — банк, зарегистрированный в соответствии с законодательством Англии и Уэльса (регистрационный № 159752), действующий на основании лицензии, выданной Управлением пруденциального регулирования, и в соответствии с требованиями, устанавливаемыми Управлением пруденциального регулирования и Службой финансовых рынков, деятельность VTB Capital plc в Сингапуре регулируется Центральным банком Сингапура (Monetary Authority of Singapore), в Дубае – Управлением финансовых услуг Дубая (DFSA). VTB Capital plc (аффилированные организации) является частью инвестиционного подразделения ПАО "Банк ВТБ". VTB Capital Hong Kong Limited лицензирован Комиссией по ценным бумагам и фьючерсам Гонконга (Hong Kong Securities and Futures Commission). Деятельность VTB Capital Inc. в США лицензирована и регулируется Управлением по регулированию финансовой отрасли (FINRA) и Комиссией по ценным бумагам и биржам США (US Securities and Exchange Commission).