АНАЛИЗ РИСКОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ КАК ЭТАП КОМПЛЕКСНОЙ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Мухин Илья Николаевич,
Всероссийская государственная налоговая академия
Министерства финансов Российской Федерации (Москва)
05.13.19
ilyuha1999@mail.ru

Аннотация. *В статье рассматривается процесс анализа рисков в управлении информационной безопасностью предприятия как этап комплексной защиты объектов информатизации.*

Ключевые слова: информационная безопасность, комплексная защита, объект информатизации, анализ рисков, управление.

THE ANALYSIS OF RISKS OF INFORMATION SECURITY MANAGEMENT OF THE ENTERPRISE AS A STAGE OF COMPLEX PROTECTION OF OBJECTS OF INFORMATIZATION

Mukhin Ilia Nikolaevich
The State Tax Academy of Russian Federation (Moscow)

Abstract. *The article deals with the analysis of risks in the management of information security of the enterprise as a stage of complex protection of objects of Informatization.*

Key words: information security, complex protection, the object of Informatization, risk analysis, management.

Введение

Как показывает опыт проведения аттестационных испытаний комплексной защиты объектов информатизации, большинство обращающихся за этой услугой весьма смутно представляют, что же такое аттестация и какие действия следует предпринять до ее начала.

Следует отметить, что процесс этот последовательный, осуществляемый в несколько этапов, по четкому алгоритму, и попытки исключить какое-то звено или поменять этапы местами приводят, как правило, к ошибкам. Их устранение потребует дополнительных (иногда существенных) затрат.

Основные этапы создания и аттестации объектов информатизации на предприятиях, в организациях, учреждениях:

1. Устанавливается предназначение создаваемого объекта информатизации (автоматизированная система – АС, выделенное помещение – ВП).
2. Определяется максимальная степень секретности обрабатываемой или обсуждаемой информации. Для АС – также и режимы обработки информации: однопользовательский, коллективный, права доступа пользователей, количество предполагаемых уровней конфиденциальности информации.
3. На основании информации, полученной в результате выполнения п. 2, устанавливается категория (для ВП и АС) и класс защиты (только для АС) от несанкционированного доступа (НСД). Результаты оформляются соответствующими актами.
4. Выбираются помещения для создаваемых объектов.

5. Проводится их обследование. Уточняется организация электропитания, расположение и сопротивление контура заземления. В ходе проверки определяются вероятные каналы утечки информации. При необходимости может проводиться инструментальный контроль, например, качества звукоизоляции ограждающих конструкций, окон, дверей ВП.
6. С учетом категории и класса ОИ, а также данных обследования осуществляется выбор и приобретение технических средств, на базе которых будет создаваться ОИ. Безусловно, при этом предпочтение должно отдаваться средствам, сертифицированным по требованиям безопасности информации или прошедшим специальные исследования и имеющим предписания на эксплуатацию.
7. В тех случаях, когда условия расположения ОИ не обеспечивают выполнение требований предписаний на эксплуатацию, выбираются дополнительные (организационные, технические, программные) средства и способы защиты информации.
8. Осуществляются установка и монтаж технических средств ОИ, в том числе средств защиты, и их настройка.
9. Разрабатывается комплект организационно-распорядительной документации по защите информации в соответствии с СТР.
10. На основании заявки в региональное управление ФСТЭК России назначается организация, имеющая аккредитацию в качестве органа по аттестации, с которой и заключается соответствующий договор на проведение аттестационных испытаний ОИ. По результатам испытаний оформляется заключение, оно согласовывается с региональным управлением ФСТЭК России. Затем составляется аттестат соответствия объекта информатизации требованиям по безопасности. Данный документ дает право обработки (обсуждения) на аттестованном объекте информации с указанной в нем степенью секретности. Срок действия аттестата соответствия – не более 3 лет.

Таков краткий алгоритм создания и аттестации объекта информатизации.

При этом очень важным звеном в этом алгоритме представляется анализ рисков при управлении информационной безопасностью предприятия, как при создании нового объекта информатизации, так и при аттестации уже существующего.

В процессе управления любым направлением деятельности предприятия необходимо вырабатывать осознанные и эффективные решения, принятие которых помогает достичь определенных целей. Адекватное решение можно принять только на основании фактов и анализа причинно-следственных связей.

С одной стороны, существует ряд стандартных подходов к решению проблем безопасности: защита периметров, защита от инсайдеров, защита от обстоятельств форс-мажорного характера, а также множество программных продуктов, позволяющих защититься от той или иной угрозы.

Однако специалисты отдела ИБ сталкиваются с тем, что выбор продуктов различного класса очень широк, информационная инфраструктура организации очень масштабна, количество потенциальных целей атак нарушителей велико, а деятельность подразделений организации разнородна и не поддается унификации. При этом каждый специалист отдела имеет собственное мнение о приоритетности направлений деятельности, соответствующее его специализации и личным приоритетам.

Определение целей и задач управления информационной безопасностью

При определении целей следует - при помощи руководства и работников организации - понять, что же на самом деле нужно защищать и от кого. Здесь начинается специфическая работа на стыке технологий и основного бизнеса, которая состоит в определении того направления деятельности и того целевого состояния обеспечения ИБ, которое будет сформулировано одновременно и в бизнес-терминах, и в терминах ИБ. Процесс анализа рисков - это и есть инструмент, с помощью которого можно определить цели управления ИБ, оценить основные критичные факторы, негативно влияющие на ключевые бизнес-процессы компании, и выработать осознанные, эффективные и обоснованные решения для их контроля или минимизации.

Цель управления ИБ состоит в сохранении конфиденциальности, целостности и доступности информации. Любое управление основано на осознании ситуации, в которой оно происходит. В терминах анализа рисков осознание ситуации выражается в инвентаризации и оценке активов организации и всего того, что обеспечивает ведение

бизнес-процессов. С точки зрения анализа рисков ИБ к основным активам относятся непосредственно информация, инфраструктура, персонал, имидж и репутация компании. Без инвентаризации активов на уровне бизнес-процессов невозможно ответить на вопрос, что именно нужно защищать. Также очень важно понять, какая информация обрабатывается в организации и где выполняется ее обработка.

В условиях крупного предприятия количество информационных активов может быть очень велико. Если деятельность предприятия автоматизирована при помощи ERP-системы, то можно говорить, что практически любому материальному объекту, использующемуся в этой деятельности, соответствует какой-либо информационный объект. Поэтому первоочередной задачей управления рисками становится определение наиболее значимых активов.

Решить эту задачу невозможно без привлечения менеджеров основного направления деятельности предприятия, как среднего, так и высшего звена. Оптимальной видится ситуация, когда высший менеджмент предприятия лично задает наиболее критичные направления деятельности, для которых крайне важно обеспечить информационную безопасность. Мнение высшего руководства по поводу приоритетов в обеспечении ИБ очень важно и ценно в процессе анализа рисков, но в любом случае оно должно уточняться путем сбора сведений о критичности активов на среднем уровне управления компанией.

Идентифицировать и локализовать информацию можно на основании описания бизнес-процессов, в рамках которых информация рассматривается как один из типов ресурсов. Задача несколько упрощается, если в организации принят подход регламентации бизнес-процессов. Формализованные описания бизнес-процессов служат хорошей стартовой точкой для инвентаризации активов. Если описаний нет, можно идентифицировать активы на основании сведений, полученных от сотрудников организации. После того как активы идентифицированы, необходимо определить их ценность.

Работа по определению ценности информационных активов в разрезе всей организации одновременно наиболее значима и сложна. Именно оценка информационных активов позволит начальнику отдела ИБ выбрать основные направления деятельности по обеспечению информационной безопасности. Ценность актива выражается величиной потерь, которые понесет организация в случае нарушения безопасности актива.

Но экономическая эффективность процесса управления ИБ во многом зависит именно от осознания того, что нужно защищать и какие затраты для этого потребуются. Здесь можно провести аналогию с классами защиты автоматизированных систем: чем значительнее риски, тем более жесткими должны быть требования к защите.

Чтобы определить последствия нарушения безопасности, нужно либо иметь сведения о зафиксированных инцидентах аналогичного характера, либо провести сценарный анализ. В рамках сценарного анализа изучаются причинно-следственные связи между событиями нарушения безопасности активов и последствиями этих событий для бизнес-процессов предприятия. Последствия сценариев должны оцениваться коллективом людей, итерационным или совещательным методом.

Если активы идентифицированы и определена их ценность, можно говорить о том, что цели обеспечения ИБ частично установлены: определены объекты защиты и значимость поддержания их в состоянии информационной безопасности для организации.

Анализ источников проблем и идентификация уязвимостей

После определения целей управления ИБ следует проанализировать проблемы, которые мешают приблизиться к целевому состоянию. На этом уровне процесс анализа рисков спускается до информационной инфраструктуры и традиционных понятий ИБ - нарушителей, угроз и уязвимостей.

Для оценки рисков недостаточно ввести стандартную модель нарушителя, разделяющую всех нарушителей по типу доступа к активу и знаниям о структуре активов. Такое разделение помогает определить, какие угрозы могут быть направлены на актив, но не дает ответа на вопрос, могут ли эти угрозы быть в принципе реализованы.

В процессе анализа рисков необходимо оценить мотивированность нарушителей при реализации угроз. При этом под нарушителем подразумевается не абстрактный внешний хакер или инсайдер, а сторона, заинтересованная в получении выгоды путем нарушения безопасности актива.

Первоначальную информацию о модели нарушителя, как и в случае с выбором изначальных

направлений деятельности по обеспечению ИБ, целесообразно получить у высшего менеджмента, представляющего себе положение организации на рынке, имеющего сведения о конкурентах и о том, каких методов воздействия можно от них ожидать. Сведения, необходимые для разработки модели нарушителя, можно получить и из специализированных исследований по нарушениям в области компьютерной безопасности в той сфере бизнеса, для которой проводится анализ рисков. Правильно проработанная модель нарушителя дополняет цели обеспечения ИБ, определенные при оценке активов организации.

Разработка модели угроз и идентификация уязвимостей неразрывно связаны с инвентаризацией окружения информационных активов организации. Доступ к информации обеспечивается при помощи информационной инфраструктуры, автоматизирующей бизнес-процессы организации. С позиции управления ИБ значимость информационной инфраструктуры может быть установлена только после определения связи между информационными активами и инфраструктурой.

В модель угроз следует включить все угрозы, выявленные по результатам смежных процессов управления ИБ, таких как управление уязвимостями и инцидентами. Угрозы необходимо будет ранжировать друг относительно друга по уровню вероятности их реализации. Для этого в процессе разработки модели угроз для каждой угрозы необходимо указать наиболее значимые факторы, существование которых оказывает влияние на ее реализацию.

После разработки модели угроз необходимо идентифицировать уязвимости в окружении активов. Идентификация и оценка уязвимостей может выполняться в рамках еще одного процесса управления ИБ - аудита. Для проведения аудита ИБ необходимо разработать критерии проверки. А критерии проверки могут быть разработаны как раз на основании модели угроз и модели нарушителя.

По результатам разработки модели угроз, модели нарушителя и идентификации уязвимостей можно говорить о том, что определены причины, влияющие на достижение целевого состояния информационной безопасности предприятия.

Оценка рисков и принятие решений

Идентифицировать и оценить активы, разработать модель нарушителя и модель угроз, идентифицировать уязвимости - это стандартные шаги, описание которых должно присутствовать в любой методике анализа рисков. Все перечисленные шаги могут выполняться с различным уровнем качества и детализации.

Полученные результаты необходимо оценить, агрегировать, классифицировать и отобразить. Так как ущерб определяется на этапе идентификации и оценки активов, необходимо оценить вероятность событий риска. Оценку вероятности можно получить на основании статистики по инцидентам, причины которых совпадают с рассматриваемыми угрозами ИБ, либо методом прогнозирования - на основании взвешивания факторов, соответствующих разработанной модели угроз.

Хорошей практикой для оценки вероятности станет классификация уязвимостей по выделенному набору факторов, характеризующих простоту эксплуатации уязвимостей. Прогнозирование вероятности угроз проводится уже на основании свойств уязвимости и групп нарушителей, от которых исходят угрозы.

Уровень риска следует определить для всех идентифицированных и соответствующих друг другу наборов «актив-угроза». При этом величина ущерба и вероятности не обязательно должны быть выражены в абсолютных денежных показателях и процентах; как правило, представить результаты в такой форме не удается. Причина этого - используемые методы анализа и оценки рисков информационной безопасности: сценарный анализ и прогнозирование.

Отчет об анализе рисков отражает следующие сведения:

- наиболее проблемные области обеспечения ИБ в организации;
- влияние угроз ИБ на общую структуру рисков организации;
- первоочередные направления деятельности отдела ИБ по повышению эффективности обеспечения ИБ.

На основании отчета об анализе рисков руководитель отдела ИБ может разработать план работы отдела на среднесрочный период и заложить бюджет исходя из характера мероприятий, необходимых для снижения рисков.

Заключение

Анализ рисков - достаточно трудоемкая процедура. В процессе анализа рисков должны применяться методические материалы и инструментальные средства. Однако для успешного внедрения повторяемого процесса этого недостаточно; еще одна важная его составляющая - регламент управления рисками. Он может быть самодостаточным и затрагивать только риски ИБ, а может быть интегрирован с общим процессом управления рисками в организации.

Одной лишь методики анализа рисков или специализированного инструментального средства для оценки рисков ИБ недостаточно. Необходимы процедуры идентификации активов, определения значимости активов, разработки моделей нарушителя и угроз, идентификации уязвимостей, агрегирования и классификации рисков.

Процесс анализа рисков непрерывен, так как верхнеуровневые цели обеспечения ИБ могут оставаться неизменными на протяжении длительного времени, а информационная инфраструктура, методы обработки информации и риски, связанные с использованием ИТ, постоянно меняться.

Анализ рисков, управление инцидентами и аудит ИБ неразрывно связаны друг с другом, поскольку связаны входы и выходы перечисленных процессов. Разработку и внедрение процесса управления рисками необходимо вести с оглядкой на управление инцидентами и аудитами ИБ.

Установление режима защиты коммерческой тайны и персональных данных неразрывно связано с анализом рисков, так как все перечисленные процессы используют сходные методы идентификации и оценки активов, разработки модели нарушителя и модели угроз.

Следовательно, анализ рисков в управлении информационной безопасностью предприятия, как при создании нового объекта информатизации, так и при аттестации уже существующего, является весьма значимым процессом для комплексной защиты объектов информатизации.

Список литературы

1. Царегородцев А.В. Мухин И.Н. Защита информационных ресурсов предприятия: Монография. – М.: ВГНА Минфина России, 2008. – 160с.
2. http://security-zone.ru - Андрей Суханов. Анализ рисков в управлении информационной безопасностью. 2009 г.