МЕТОДОЛОГИЯ ПРИМЕНЕНИЯ ИНТЕГРИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ УГРОЗАМИ

Егоров М.А. Email: Egorov665@scientifictext.ru

Егоров Максим Александрович – магистрант,
институт информационных наук,
Московский государственный лингвистический университет, г. Москва.

Аннотация: *за последние 20 лет появилось огромное множество технологий, которые изменили и продолжают кардинально изменять окружающий нас мир, цифровой мир в полном размахе конвергируется с материальным миром: мы отходим от печатных документов к электронным, покупаем билеты в онлайн-версии, оплачиваем покупки, используя не наличные средства, а безналичные. В наше время все уже привыкли получать зарплату и пенсию на счета в банках и управлять ими с помощью онлайн-клиентов, портативные-терминалы и банкоматы находятся в двух шагах от дома и места работы. Ежедневно обладатели дебетовых и кредитных карт задаются вопросом безопасности своих цифровых средств на своих счетах, и это происходит из-за одной главной причины: с каждым днем злоумышленники придумывают и осуществляют новые методы и технологии хищения персональных, секретных и банковских данных, а потеря или утечка этих данных вызывают финансовые, временные и материальные затраты для ликвидации последствия угроз. В наше время аудит информационной безопасности позволяет провести и предоставить полную и наиболее объективную оценку защищенности ИС, выявить наличие проблем и разработать подходящую и наиболее эффективную программу для построения СОИБ организации. В рамках аудита ИБ или рамках отдельного процесса может быть проведен тест на проникновение, позволяющий проверить способность ИС компании противостоять попыткам проникновения в сеть и неправомочного воздействия на информацию, но, к сожалению, в постоянно меняющееся время информационная система должна также быть способной противостоять угрозам и в лучшем случае нейтрализовать их.*

Ключевые слова: *информационная безопасность, аудит информационной безопасности, угрозы, система управления угрозами.*

METHODOLOGY ON THE APPLICATION OF INTEGRATED MANAGEMENT SYSTEM THREATS

Egorov M.A.

Egorov Maxim Aleksandrovich – Master,
INSTITUTE OF INFORMATION SCIENCE,
MOSCOW STATE LINGUISTIC UNIVERSITY, MOSCOW

Abstract: *over the past 20 years, a huge variety of technologies have appeared that have changed and continue to radically change the world around us, the digital world is converging on a full scale with the material world: we move away from printed documents to electronic, buy tickets online, pay for purchases using not cash but cards. Nowadays, everyone is used to receive salary and pension on Bank accounts and manage them with the help of online clients, portable terminals and ATMs are a stone's throw from home and place of work. Every day, debit and credit cardholders wonder about the security of their digital funds in their accounts, and this is due to one main reason: every day attackers come up with and implement new methods and technologies of theft of personal, secret and banking data, and the loss or leakage of these data cause financial, time and material costs to eliminate the consequences of threats. Nowadays, information security audit allows you to conduct and provide a complete and most objective assessment of the security of information systems, to identify problems and develop the most appropriate and effective program for building an information security system of the organization. As part of an information security audit or as part of a separate process, a penetration test can be conducted to verify the company's ability to resist attempts to penetrate the network and unauthorized impact on information, but, unfortunately, in an ever-changing time, the information system must also be able to withstand threats and, at best, neutralize them.*

Keywords: *information security, information security audit, threats, threat management system.*

УДК 007.51

В данной статье будет представлена разработанная методология применения интегрированной системы управления (нейтрализации) угроз (СУУ) для создания базы по нейтрализации их. При её разработке, было решено дополнить существующие методики обеспечения защищенности

информационных систем, путем описывания основных подходов к управлению угрозами и процедурами управления ими/их нейтрализации.

Под управлением угроз, подразумевается процесс, при котором осуществляется обнаружение, предупреждение и последующий контроль угроз, основанный на доработки системы, путём автоматизирования существующих средств обеспечения информационной безопасности до приемлемого уровня, на котором система способна их обнаружить и применить меры/действия для их нейтрализации без участия человека.

Задачей является предложить механизмы унификации и эффективной организации процесса управления угрозами в Компании для нейтрализации их. Разрабатывая данную методологию, не ставилось главной целью охватить все возможные сценарии, которые могут возникнуть в процессе применения СУУ, предполагая, что процесс управления угрозами, являясь частью ежедневного процесса управления, должен предоставлять определенную свободу применения различных стилей управления и творческого подхода. Более того данная методология должна регулярно обновляться и совершенствоваться с тем, чтобы отражать постоянно накапливающийся опыт Компании и передовую практику в области управления угрозами.

СУУ должна рассматриваться в качестве инструмента, поддерживающего операционную деятельность Компании, а не в качестве обособленного и самодостаточного процесса. Поэтому она должна стать неотъемлемой частью уже существующих в компании организационно-технически-технологических форм управления и процессов, включая регулярные процедуры оценки результатов деятельности и другие аналогичные процедуры.

Классификация угроз

Угрозы, существующие как внутри компании, так и вне её систематизированы по следующим признакам:

- Их потенциальное влияние на процесс функционирования компании;
- Уровень руководителей и заинтересованных лиц, участвующих в мониторинге и контроле за угрозами.

Угрозы 1-го уровня

Угрозы 1-го уровня – это угрозы, представляющие настолько серьезную угрозу для развития и функционирования информационных систем компании, что они подлежат постоянному мониторингу и контролю со стороны администраторов информационной безопасности. В зависимости от их влияния данные угрозы подразделяются на основные и прочие угрозы.

В функциональном отношении данные угрозы разбиты на следующие категории:

- Угрозы, направленные на дестабилизацию управления организацией/информационными системами
- Угрозы, направленные на дестабилизацию производственных процессов
- Угрозы, направленные на дестабилизацию финансового обеспечения компании
- Угрозы репутации
- Угрозы, направленные на активность инвестиционной деятельности.

Угрозы 2-го уровня

Угрозы 2-го уровня – угрозы, в отношении которых можно осуществлять мониторинг, контроль и управление на уровне конкретного бизнес-функционального процесса, несмотря на то, что данные угрозы свойственны деятельности всей компании в целом.

Классификация угроз 2-го уровня выполняется отдельно существующими владельцами бизнес-процессов.

Угрозы 3-го уровня

Угрозы 3-го уровня – угрозы, направленные на бизнес-единицы и процессы, представляют собой угрозы, которые присущи функционированию отдельных бизнес единиц и могут быть предметом мониторинга, контроля и управления на уровне каждой бизнес-единицы. При необходимости данные угрозы могут быть сгруппированы в угрозы бизнес-функционального процесса.

Внутренняя среда

Компания стремится задать надлежащий тон процессу управления угрозами на всех уровня организации и во всех её функциональных подразделениях. Внутренняя среда определяет подходы и отношение персонала к угрозам и включает:

Философия управления угрозами – позволяет получить общее представление об управлениями угрозами и понять его роль и важность для деятельности компании; быть готовыми к возможным угрозам и знать, как поступать в случае их возникновения; вести постоянный поиск новой информации о передовом опыте в области управления угрозами, включая опыт конкурентов и предприятий других отраслей промышленности, и обмениваться этой информацией внутри Компании;

Приемлемый уровень реагирования и нейтрализации угроз – гарантирует, что каждой угрозе уделяется должное внимание; ни одна угроза не упускается из виду, даже если не представляется

возможным дать точное количественное определение параметров; имеющиеся ресурсы используются эффективным образом, поскольку не создаются искусственные или неразумные ориентиры и показатели там, где наиболее полезными являются здравый смысл и накопленный опыт корпоративной деятельности;

Культура управления угрозами – подразумевает, что компания внедряет и использует подход, основанный на угрозах, в отношении всех видов своей деятельности; процесс управления угрозами тесно связан с процессами планирования и управления эффективностью деятельности компании; управление угрозами должно являться частью регулярных отчетов, а также обсуждаться на встречах; ответственные руководители персонально отвечают за общую эффективность и результативность процесса управления угрозами.

Выявление угрозы

Процесс выявления угроз может быть связан с одним из следующих событий:

1) Первоначальное выявление угрозы (обнаружение новых угроз для разработки стратегии реагирования)
2) Инвентаризация угроз (ежегодный анализ портфеля угроз)
3) Обнаружение потенциальных угроз (случайно обнаружение новых потенциальных угроз в ходе нормальной деятельности, не включаются в портфель автоматически, но прежде анализируются на предмет возможного дублирования других угроз портфеля)

В отношении первых двух случаев применяются одинаковые процедуры, в то время как в последнем из перечисленных случаев используется специальный подход. Выявление угроз и их оценка представляют собой два последовательных этапа процесса управления угрозами, однако на практике они обычно осуществляются одновременно в ходе выполнения одних и тех же процедур.

Целью процедуры первоначального выявления угрозы состоит в обнаружении новых угроз для их последующей оценки, выработки надлежащей стратегии реагирования и совершенствования информационной системы для их нейтрализации.

Регулярная инвентаризация угроз призвана выявить среди ранее обнаруженных такие угрозы, которые в настоящий момент можно классифицировать как «неактивные», то есть вероятность их появления близка к нулю.

Целью процедуры обнаружения потенциальных угроз состоит в том, чтобы привлечь внимание заинтересованных лиц с в сфере информационной безопасности к информации, которая может указывать на появление новых угроз или существенных изменений в значимости угроз.

Подход к выявлению угроз

Выявление и инвентаризация угроз могут осуществляться посредством ряда процедур, например:

- Обсуждение угроз в ходе проведения собраний заинтересованных лиц и прочих регулярных встреч
- Специальные семинары по управлению угрозами с целью выявления/инвентаризации угроз
- Объединенные заседания
- Обнаружение потенциальных угроз персоналом компании

Наиболее практичной и эффективной формой выявления и инвентаризации угроз и оценки портфеля угроз являются семинары, проводимые с участием опытных и знающих специалистов. Такие мероприятия организуются либо внутри компании, либо вне её. Для повышения эффективности и результативности обсуждений, касающихся выявления и инвентаризации угроз, заинтересованным лицам рекомендуется заранее изучить и обдумать следующие вопросы:

- Текущий статус информационных систем и связанных с ними угроз
- Предыдущий практический опыт участников
- Позитивный и негативный опыт других организаций и предприятий
- Усвоенные уроки
- Гипотетические ситуации, в результате которых могут возникнуть новые угрозы
- Другая информация, относящаяся к предмету обсуждения.

В зависимости от количества и масштаба рассматриваемых угроз, обсуждение может проводиться в ходе не одного, а ряда подобных семинаров.

Рекомендованный подход к обнаружению потенциальных угроз

В рамках данного подхода, персонал может участвовать в выявлении новых потенциальных угроз. При выполнении своих ежедневных обязанностей сотрудник может заметить признаки появления новой угрозы или существенного изменения значимости угрозы. В таком случае, сотруднику рекомендуется передать такую информацию соответствующим заинтересованным лицам по угрозам путем заполнения Оперативного отчета о угрозе.

Перед подачей Оперативного отчета о угрозе, сотруднику, занимающемуся исследованием новой или возросшей угрозы, рекомендуется:

- Удостовериться, что вновь выявленная информация может способствовать появлению новой угрозы в Регистре угроз или повлиять на рейтинг ранее выявленной угрозы;
- Обратиться за помощью к заинтересованным лицам по угрозам, чтобы определить, какую информацию следует включить в Оперативный отчет о угрозе.

Несмотря на то, что Оперативный отчет о угрозе не должен включать в себя полное описание угрозы, в нем, тем не менее, должна содержаться достаточная информация для того, чтобы пользователь отчета смог сделать предварительные выводы в отношении:

- Надежности показателей появления/изменения угрозы;
- Потенциальных последствий реализации угрозы для бизнес-процессов и деятельности Компании.

Результатом процесса выявления и инвентаризации угроз должна быть выработка заключений по следующим вопросам:

- Новые угрозы, если выявлены
- Пересмотр ранее выявленных угроз, определение среди них «неактивных»
- Для каждой угрозы
  - Краткое наименование угрозы
  - Источник угрозы
  - Факторы и условия возникновения угрозы
  - Угроза
  - Последствия реализации угрозы
  - Требуемый результат
  - Взаимосвязь с другими угрозами
  - Возможные подходы к управлению угрозами

Вышеперечисленные характеристики угроз, а также результаты их оценки вносят в стандартную форму Отчета о угрозе. Посредством использования автоматических настроек или доработки программ и сценариев по нейтрализации угроз появляется возможность обновить информацию в соответствующих системах для того, чтобы системы были готовы осуществить их нейтрализацию.

Сроки

В случае первоначального выявления угроз сроки проведения процедур согласовываются с ответственным руководителем, возглавляющим процесс внедрения системы управления угрозами.

Регулярная инвентаризация угроз должна проводиться в сроки, позволяющие своевременно подготовить и модернизировать систему по реагированию на угрозы.

Обнаружение потенциальной угрозы является постоянной процедурой, следовательно, у неё нет сроков. Тем не менее, в общем случае обработки получаемой информации, должна обеспечиваться возможность адекватного и своевременного реагирования на потенциальную угрозу.

Оценка угроз

Нумерация квадратов представляет собой, в сущности, рейтинг угроз, на основе которого производится ранжирование угроз с целью акцентировать внимание членов Рабочей группы на более значимых угрозах и правильно распределить ресурсы для осуществления противодействия и предупреждения им.

Главной целью оценки угроз заключается в их ранжировании. Это позволяет обоснованно распределить и не допустить перерасхода ресурсов в связи с управлением всей совокупностью потенциальных угроз.

Степень влияния угрозы	Балл влияния	Значимость угрозы									
Высокая	3	3	6	9	12	15	18	21	24	27	30
Средняя	2	2	4	6	8	10	12	14	16	18	20
Низкая	1	1	2	3	4	5	6	7	8	9	10
		1	2	3	4	5	6	7	8	9	10
		Баллы вероятности угрозы									
Вероятность угрозы		Низкая			Средняя			Высокая			

Значимость угрозы	
Высокая	Существенный ущерб угрозы для информационной системы
Средняя	Средний ущерб угрозы для информационной системы
Низкая	Несущественный ущерб угрозы для информационной системы

Рис. 1. Таблица. Классификация угроз по значимости

Процедура оценки угроз предусматривает определение значимости угроз с целью дальнейшего ранжирования портфеля угроз по этому признаку. Кроме того, необходимо оценить степень управляемости угроз с тем, чтобы впоследствии разработать наиболее обоснованные и эффективные планы по реагированию на них.

Значимость угрозы представляет собой произведение вероятности угрозы и её влияния последствий (ущерба).

Зу = Ву * Уу

Как вероятность, так и последствия от угрозы могут оцениваться тремя способами, описанными ниже:

Количественная оценка – вероятность и последствия действий угрозы выражаются либо в качестве точных числовых показателей, например 15%, 80 тыс. рублей, либо в качестве простого распределения, например, минимум =5%, вероятно = 15%, максимум = 40%. Не всегда легко сделать точное предположение в отношении как вероятности, так и последствий определенной угрозы. Необходимо сопоставлять производимые при этом затраты (времени и ресурсов) с преимуществами, получаемым от точной оценки. Однако, когда точное значение вероятности и последствий угрозы легко определить или если это важно для оценки рентабельности мероприятий по реагированию на угрозы, следует применять количественную оценку.

Полуколичественная оценка – вероятность и последствия выражаются при помощи интервала значений, например 5%-15%, 100 тыс. рублей – 500 тыс. рублей. Полуколичественная оценка является рекомендуемым методом определения последствий и вероятности угрозы, поскольку в большинстве случаев она позволяет оптимизировать соотношение затрат на проведение оценки и получаемых от неё преимуществ.

Качественная оценка – при данном способе используются определения, напрямую не связанные с финансовыми показателями, например, высокий. Качественная оценка применяется для быстрого определения угроз, не являющихся значимыми с тем, чтобы в дальнейшем исключить их из процесса детального рассмотрения.

Что касается более существенных угроз, то по отношению к ним следует в максимальной степени применять количественный или полуколичественный подход, чтобы четко понять потенциальные последствия каждой конкретной угрозы для деятельности Компании и убедиться в самом факте существования угрозы.

Все три вышеперечисленных подхода применимы к оценке как финансовых, так и нефинансовых угроз, причем в большинстве случаев последствия угрозы содержит в различных процедурах как финансовый, так и нефинансовый компоненты.

В ходе анализа угроз не следует концентрироваться исключительно на текущих условиях, но необходимо уделять должное внимание возможным будущим событиям, способным оказать влияние на стратегическое развитие компании. Таким образом, анализ угроз должен охватывать период времени в будущем, по меньшей мере равный тому, на который планируется разработка системы для нейтрализации угроз.

Таблица 1. Критерии оценки вероятности угрозы

Степень вероятности	Качественные критерии	Количественные критерии	Частота проявления
Высокая	Очень высокая 5	Более 1 из 5	Чаще 1 раза в неделю
	Высокая 4	Более 1 из 50	Чаще 1 раза в месяц
Средняя	Умеренная 3	Более 1 из 500	Чаще 1 раза в квартал
Низкая	Низкая 2	Более 1 из 5000	Чаще 1 раза в год
	Малая 1	Менее 1 из 5000	Реже 1 раза в год

После оценки угрозы размещаются на Матрице оценки угроз. Посредством представления вероятности и последствий угроз согласно принятой шкале Матрица оценки угроз:

- Способствует общему пониманию по управлению угрозами относительной важности каждой угрозы;
- Предоставляет основу для ранжирования угроз в целях планирования действий по реагированию на них;
- Дает наглядное графическое представление о портфеле угроз, которое может служить основой для последующих обсуждений.

Угрозы размещаются на Матрице оценки угроз в зависимости от значений их последствий и вероятности, как это показано на таблице.

Оценка управляемости представляет собой следующий шаг процедуры оценки угроз и позволяет определить, способна ли Компания привести остаточный уровень угрозы к приемлемому уровню и обладает ли она достаточными для этого ресурсами, или же Компания не способна воздействовать на факторы, способствующие появлению угрозы. Управляемость оценивается на основе качественного подхода с применением критериев представленных на таблице.

Таблица 2. Степень управляемости

Степень управляемости	Комментарий
Очень высокая 5	Банк может полностью контролировать угрозу и оказываемое ею влияние
Высокая 4	Банк может значительно контролировать угрозу и оказываемое ею влияние
Средняя 3	Банк может воздействовать на угрозу и оказываемое ею влияние
Умеренная 2	Банк может воздействовать на угрозу и оказываемое ею влияние
Низкая 1	Банк не может видит угроз и не способен отследить её влияние

Сроки

Процедура оценки угроз проводится одновременно с процедурой их выявления.

3.4 Реагирование на угрозы

Определение стратегии реагирования на угрозу и разработка соответствующих алгоритмов – это ключевой этап, переводящий процесс управления угрозами из фазы «Они есть» в фазу «Они управляются».

Стратегии реагирования на угрозу могут быть следующими:

- УУ - Уменьшение уровня угрозы – уменьшение потенциальных последствий или снижение вероятности его возникновения, либо того и другого. Стратегия уменьшения уровня угрозы предназначается только для угроз с остаточным уровнем управляемости.
- ПЧС - Планирование чрезвычайных ситуаций – снижение последствий от воздействия угрозы путем разработки ряда краткосрочных мероприятий, которые должны заблаговременно доводиться до сведения администраторов и выполняться непосредственно после происшествия (если таковое происходит). Планирование чрезвычайных мероприятий может применяться как в отношении угроз с низким уровнем управляемости, так и в отношении других угроз, потенциально имеющих высокую степень влияния.

Таблица 3. Планы действий для предотвращения угроз информационной безопасности в информационной системе

<table>
<tr><td>Значимость</td><td>Балл</td><td colspan="5"></td></tr>
<tr><td rowspan="3">Высокая</td><td>15</td><td rowspan="3">ПЧС + (ПД)</td><td>ПД + (ПЧС)</td><td rowspan="3">ПД + (ПЧС)</td><td rowspan="3">ПД</td><td rowspan="6">ПД</td></tr>
<tr><td>12</td><td rowspan="2">ПЧС + (ПД)</td></tr>
<tr><td>10</td></tr>
<tr><td rowspan="5">Средняя</td><td>9</td><td rowspan="5">ПД или ПЧС</td></tr>
<tr><td>8</td><td rowspan="3">ПД или ПЧС</td></tr>
<tr><td>6</td></tr>
<tr><td>5</td><td rowspan="3">ПД + (ПЧС)</td></tr>
<tr><td>4</td><td rowspan="2">ПД или ПЧС</td></tr>
<tr><td rowspan="3">Низкая</td><td>3</td><td rowspan="3">ПЧС</td></tr>
<tr><td>2</td><td>ПЧС</td></tr>
<tr><td>1</td></tr>
<tr><td colspan="2"></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td colspan="2"></td><td colspan="5">Баллы управляемости</td></tr>
<tr><td colspan="2">Управляемость</td><td>Низкая</td><td>Умерен.</td><td>Средняя</td><td>Высокая</td><td>Очень высокая</td></tr>
</table>

- ПКЗ - Передача контроля за угрозами – передача потенциальных последствий, связанных с угрозой, третьей стороне, обладающей возможностью контролировать данную угрозу. При этом важно понимать, что угрозы не могут передаваться третьим сторонам полностью, так как всегда существует остаточная угроза, либо возникают другие угрозы. Тем не менее, передача контроля за угрозами может стать эффективной стратегией реагирования на угрозу при условии, что остаточные угрозы оцениваются как приемлемые.
- ОКУ - Отказ от контроля за угрозой – прекращение деятельности, связанной с угрозой. Эта стратегия обычно используется в отношении угроз, несущих в себе угрозу непрерывности деятельности компании.
- ПУ - Принятие угрозы – стратегия, в рамках которой не предусматривается каких-либо специальных действий в отношении определенной угрозы. Обычно данная стратегия, применима в случаях, когда уровень значимости угрозы до осуществления специальных мер по его снижению не превышает приемлемого уровня.

Согласований стратегий реагирования на угрозы и детальных мероприятий в рамках таких стратегий может осуществляться посредством следующих процедур:

- Действия по реагированию на угрозу (План действий по управлению угрозой и План чрезвычайных мероприятий) разрабатываются соответствующими заинтересованными лицами либо владельцем процесса и согласовываются со всеми;
- Действия по реагированию на угрозу разрабатываются в ходе заседаний по управлению угрозами, подтверждаются заинтересованными лицами и владельцем процесса.
- Действия по реагированию на угрозу разрабатываются совместно с несколькими бизнес-направлениями и функциональными подразделениями, вовлеченными в соответствующие процессы, и подтверждаются владельцем процесса или заинтересованными лицами.

Действия по реагированию на угрозу включают следующее:

- План действий по управлению угрозой (обязателен для всех существующих угроз)
- План чрезвычайных мероприятий (при необходимости)

Планы действий по управлению рисками и Планы чрезвычайных мероприятий могут обновляться и изменяться, в них могут вноситься дополнения, часть мероприятий может быть отменена, могут быть совмещены сроки их выполнения. Факт и причины внесения изменений должны быть зафиксированы в документах и согласованы со всеми лицами.

Сроки

Реагирование на угрозы является непрерывным процессом и ежеквартально или ежемесячно должен дорабатываться.

Информация об угрозах и её представление

Цели данного элемента СУУ состоят в следующем:

- Обеспечение максимальной автоматизации процесса обмена информацией в рамках СУУ и автоматизации процессов СУУ.
- Предоставление адекватной обратной связи в отношении переданной информации
- Выполнение требований к конфиденциальности

Мониторинг и обучение

СУУ предусматривает механизмы, призванные определить, продолжает ли существующий процесс управления угрозами нести в себе ценность с точки зрения повышения эффективности деятельности Компании. Эти механизмы включают как регулярные, так и разовые мероприятия, например:

Постоянный мониторинг со стороны заинтересованных лиц - является частью нормальной повседневной деятельности Компании, осуществляется в режиме реального времени и помогает более динамично реагировать на изменяющиеся условия. Для отслеживания эффективности ИСУР могут использоваться различные повседневные мероприятия, осуществляемые в рамках обычного управления Компанией, в том числе регулярные процедуры управления и надзора, анализ отклонений, стресс-тестирование, сравнение, согласование данных и другие рутинные процедуры. Ответственные руководители несут ответственность за проведение регулярных мероприятий по мониторингу ИСУР в подчиненных им подразделениях, а также за принятие соответствующих управленческих решений;

- Обучение, основанное на угрозах - постоянный процесс обучения, основанного на угрозах, в значительной степени отражает внутреннюю среду Компании, а также то, как СУУ рассматривается работниками Компании на разных уровнях. Обучение, основанное на угрозах, может быть реализовано посредством регулярных неформальных обсуждений различных вопросов, касающихся угроз, в широком кругу работников Компании. Среди прочего, возможные темы могут включать: приобретенный опыт; успешные примеры управления угрозами; внешний опыт управления угрозами, сравнения с другими компаниями; внешние примеры передового и негативного опыта, демонстрируемые как представителями той же отрасли промышленности, так и компаниями из других отраслей; обмен знаниями и опытом управления угрозами между различными подразделениями Компании;
- Надзор со стороны третьей стороны – третья сторона осуществляет надзор за процессом СУУ в целом и, если сочтет это необходимым, за процессом управления отдельными угрозами;
- Оценка внутренними аудиторами - как правило, механизмы постоянного контроля предоставляют важную информацию об эффективности СУУ Компании. В дополнение к этому, важно периодически менять «угол зрения» с целью проверки соответствия процесса ожиданиям, а также определения и устранения возможных недостатков. Комитет по аудиту может поручать проведение детального анализа и оценки СУУ внутренним аудиторам. Такая контрольно-оценочная деятельность может варьироваться в своем масштабе и периодичности. Первоочередные угрозы и меры по управлению ими обычно предполагают более частые проверки. Всеобъемлющая оценка СУУ, как правило, требуется не так часто, как проверка отдельных ее областей, но все же может потребоваться по целому ряду причин: значительные изменения в области стратегии или управления, приобретение или отчуждение значительных активов, серьезные экономические или политические перемены и т.д. Методы и инструменты проверки, применяемые внутренними аудиторами, могут включать перечни контрольных вопросов, опросные листы, графические схемы процессов, различные технологии сравнения с эталонами и т.д. Выявляемые недостатки обсуждаются с руководством проверяемого подразделения и требуют представления внутренними аудиторами рекомендаций, направленных на их устранение. Руководство проверяемого подразделения, в свою очередь, разрабатывает и согласовывает с внутренними аудиторами план действий, направленный на устранение недостатков и внедрение рекомендаций. Отчет по результатам проверки подписывается Главным аудитором и соответствующим образом передается Спонсору проверки. Факт отсутствия недостатков также должен отражаться в отчете.
- Оценка внешними аудиторами - Подобно вышеупомянутым проверкам внутренними аудиторами, проверка СУУ может поручаться и внешним аудиторам. Спонсор проверки определяет ее цели и масштаб, а также необходимый формат отчета. Комитет ПО аудиту Совета Директоров утверждает запрос о проведении проверки СУУ и участвует в отборе внешнего аудитора. Критерии отбора внешнего аудитора зависят от целей и масштаба проверки.

Таким образом в данной главе была представлена методология применения системы управления угрозами. Были рассмотрены такие важные этапы, как классификация угроз, выявление и подход к выявлению угроз, оценка угроз, реагирование на угрозы, а также осуществление мониторинга угроз и обучение персонала.

Тем самым она может послужить основой для осуществления нейтрализации угроз и решения актуальных вопросов аудита информационной безопасности.

Список литературы / References

1. *Турбанов А., Тютюнник А.* Банковское дело. Операции, технологии, управление. И: Альпина Паблишер, 2010. 682 с.
2. Угрозы информационной безопасности и условия ее правового обеспечения. Дербин Е.А, 2015.
3. Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства. ФГАОУ ВПО «Волгоградский государственный университет», 2015.