МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: УПРАВЛЕНИЕ РИСКАМИ

***Дорофеев Александр Владимирович**, CISSP, CISA*

Публикация продолжает серию статей для специалистов по информационной безопасности, готовящихся сдать экзамен на получение статуса CISSP (Certified Information Systems Security Professional). На примере рассмотрены базовые принципы управления рисками информационной безопасности.

***Ключевые слова**: сертификация специалистов, CISSP, система менеджмента информационной безопасности (СМИБ), управление рисками информационной безопасности.*

INFORMATION SECURITY MANAGEMENT: RISK MANAGEMENT

***Alexander Dorofeev**, CISSP, CISA*

Publication continues the series of articles devoted to preparation for the CISSP (Certified Information Systems Security Professional) exam. Basic concepts of information security risk management are examined on the real case.

***Keywords**: experts certification, CISSP, information security management system (ISMS), risk management.*

Продолжая рассматривать вопросы менеджмента информационной безопасности в настоящей статье, разберем этапы процесса *управления рисками информационной безопасности* [1, 2]. Мы будем оценивать и минимизировать риски информационной безопасности на примере, прообразом которого послужил реальный случай из практики.

Управление рисками информационной безопасности по своей сути является ядром системы менеджмента информационной безопасности (СМИБ). Составляющими процесса управления рисками являются процедуры своевременного выявления рисков (risk identification), их оценка (risk assessment) и последующая обработка (risk treatment) [3].

Чтобы подробно разобрать основные этапы процесса управления рисками, рассмотрим следующую ситуацию. Крупная компания-производитель стирального порошка собирается провести промо-акцию, в ходе которой должен быть развернут веб-ресурс, на котором участники акции будут регистрировать специальные коды, указанные на упаковке продукции. В качестве призов выбраны спортивные автомобили известной итальянской марки. Счастливыми обладателями дорогих автомобилей должны стать покупатели, которые зарегистрируют свои купоны и по счету их купоны будут соответственно 500, 10 000 или 100 000. Компания не хочет, чтобы мошенники завладели одним или несколькими призами. Нас привлекают в качестве экспертов по информационной безопасности для проведения оценки рисков и формирования рекомендаций по выбору контролей.

Чтобы не изобретать велосипед, перед созданием собственной методики оценки рисков нам стоит заглянуть в международный стандарт ISO/IEC 27001:2013 и посмотреть, какие требования к методике в нем определены.

В первую очередь стандарт требует от нас формализации процесса оценки рисков для того, чтобы применяя разработанную методику, мы могли получать сравнимые результаты.

В отличие от предыдущей версии стандарта (2005 года) в новом стандарте описание данных процессов достаточно общее. Стандартом предусмотрены лишь основные этапы оценки рисков такие как, идентификация рисков информационной безопасности, анализ рисков информаци-

онной безопасности, ранжирование рисков по степени критичности.

Исходя из практического опыта, стоит отметить, что любая хорошо продуманная методология оценки рисков информационной безопасности предусматривает такие шаги, как:

- выявление угроз, направленных на рассматриваемые активы;
- определение последствий от реализации угроз;
- выявление уязвимостей;
- выявление существующих контролей (контрмер);
- определение вероятности реализации угроз.

Как видим, шаги методики определяются, исходя из определения понятия риска. Читатели предущей нашей статьи, конечно, помнят, что риск определяется, как комбинация вероятности реализации угрозы и последствий. Соответственно и мы будем определять релевантные угрозы, оценивать вероятность их реализации и размер ущерба.

Шаг 1. Определение критериев оценки

До применения каких-либо ша гов по оценке рисков, мы должны определить критерии для их оценки.

Один из подходов, позволяющих определить критерии для оценки последствий, заключается в том, чтобы оттолкнуться от целей, которые мы ставим перед информационной безопасностью. Как вы помните, защитой информации мы занимаемся для того, чтобы минимизировать финансовые потери, сохранить или даже улучшить имидж организации, а также выполнить требования регуляторов (при желании список, конечно, можно продолжить). Соответственно, и в нашем случае, мы определяем и согласовываем с заказчиком следующие уровни:

Уровень Последствий (I)	Финансовые потери	Удар по имиджу	Проблемы с регуляторами
Высокий (В)	Более 500 тыс. руб.	Аудитория сообщения, содержащего негативную, информацию более 1 млн. чел. Например, сюжет в выпуске новостей на федеральном телеканале.	Отзыв лицензии.
Средний (С)	От 100 тыс. до 500 тыс. руб.	Аудитория сообщения, содержащего негативную, информацию от 10 тыс. чел до 1 млн. чел. Например, публикация негативной заметки на страницах популярного блога с последующим распространением на других ресурсах.	Штраф за нарушение.
Низкий (Н)	Менее 100 тыс. руб.	Аудитория сообщения, содержащего негативную, информацию менее 10 тыс. чел. Например, негативный отзыв на сайте организации.	Предупреждение.

В случае если реализация угрозы приводит к различным видам последствий и разного уровня, то мы будем выбирать максимальный уровень.

Для оценки вероятности реализации угроз мы сознательно ограничимся следующими критериями: имеющаяся статистика по аналогичным инцидентам, требуемые затраты на реализацию угрозы и возможность обнаружения.

Важно отметить, что если бы в нашем случае речь шла не о разрабатываемой системе, а о существующей, то на вероятность реализации угрозы также влияли ли бы такие факторы, как наличие уязвимостей и отсутствие, либо неэффективность контролей (контрмер).

Теперь можно создать таблицу, в которой сопоставить вероятность реализации угрозы с размерами ее последствий и получить значения рисков.

Вероятность	Статистика инцидентов	Затраты на реализацию угрозы	Возможность обнаружения
Высокая (В)	Аналогичный инцидент происходит в организации каждую неделю.	**Финансовые затраты:** менее 10 тыс. руб. **Интеллектуальные:** невысокая квалификация злоумышленника. **Инструменты для реализации угрозы** общедоступны.	Угрозу и ее источник очень сложно обнаружить.
Средняя (С)	Аналогичный инцидент происходит в организации каждый месяц.	**Финансовые затраты:** от 10 тыс. до 100 тыс. рублей. **Интеллектуальные:** средняя квалификация злоумышленника. **Инструменты для реализации угрозы** можно приобрести или создать за разумный срок.	Угрозу и ее источник можно вычислить, но для этого потребуются серьезные усилия.
Низкая (Н)	Аналогичный инцидент происходит в организации каждый год.	**Финансовые затраты:** менее более 100 тыс. рублей. **Интеллектуальные:** высокая квалификация злоумышленника. **Инструменты для реализации угрозы** на данный момент не доступны.	Угроза и ее источник легко обнаруживается.

Последствия / Вероятность	Н	С	В
Н	Н	Н	С
С	Н	С	В
В	С	В	В

Шаг 2. Идентификация рисков

После того, как мы определили критерии, которые мы будем использовать для оценки рисков, в соответствии с требованиями ISO 27001:2013, нам необходимо идентифицировать угрозы и, соответственно, риски.

Прежде чем бросаться в бой и формировать список рисков, проанализируем, кто или что может выступить в качестве источника угроз. В нашем случае такими источниками могут быть:

- разработчик системы,
- администратор датацентра, на площадке которого размещается веб-ресурс,
- администратор компании-организатора акции,
- внешний злоумышленник (хакер),
- недобросовестный участник акции.

Зафиксируем в следующей таблице, что плохого они могут сделать:

№	Источник угрозы	Угрозы
1	Разработчик системы	• Внесение логической закладки. Например, как только в таблицу вносится запись под номером 499, добавляется следующая выигрышная запись с именем знакомого подставного лица. • Ошибки программирования, ведущие к уязвимостям системы. Например, отсутствие фильтрации данных вводимых пользователем в форму регистрации, приводящая к возможности реализации атаки SQL-инъекции
2	Администратор датацентра (доступ к ОС, СУБД отсутствует)	• Перехват и анализ трафика сервера акции с целью подсчета регистраций и регистрации в нужный момент «своего» купона.
3	Администратор компании-организатора акции	• Перехват и анализ трафика сервера акции с целью подсчета регистраций и регистрации в нужный момент «своего» купона. • Внесение в таблицу базы данных, используемых сайтом, записи с данными подставного лица.
4	Внешний злоумышленник (хакер)	• Взлом сайта. Например, для того, чтобы получить права администратора. • Внесение в таблицу базы данных, используемых сайтом, записи с данными подставного лица. • Проведение DDoS-атаки
5	Недобросовестный потребитель	• Регистрация купонов в большом количестве (нарушение условий акции).

Стоит отметить, что мы ограничили перечень угроз наиболее реальными (например, мы не рассматриваем угрозу падения метеорита на датацентр), также мы не спускаемся на неадекватный уровен детализации (например, отказ какой-либо микросхемы, размещенной на материнской плате сервера). Конечно, можно подобные подходы упрекнуть в том, что анализ будет не полным, но в данном случае лучше иметь неполный анализ, чем впасть в так называемый «паралич от анализа», потратив большие ресурсы на оценку того, что никак не повлияет на ситуацию.

Шаг 3. Оценка рисков

Теперь попробуем оценить вероятность и последствия угрозы и соответственно определить значение риска.

N	Угроза	Оценка вероятности	Комментарии к оценке	Оценка последствий	Комментарии к оценке	Риск
T1	Внесение логической закладки	C	Требуется средняя квалификация. Авторство закладки можно вычислить в виду ограниченного круга разработчиков.	B	Потеря автомобиля (ей).	B
T2	Ошибки программирования, ведущие к уязвимостям системы	H	Опытная команда разработчиков, аналогичные инциденты с данной командой происходят не чаще одного раза в год	B	Потеря автомобиля в случае, если внесенная уязвимость действительно опасная	C
T3	Перехват и анализ трафика сервера акции с целью подсчета регистраций и регистрации в нужный момент «своего» купона	B	Доступны свободно-распространяемые средства перехвата трафика. Выявить наличие перехвата трафика непросто.	B	Потеря одного автомобиля. Злоумышленники будут целиться в данном случае на первую выигрышную регистрацию.	B
T4	Внесение в таблицу базы данных, используемых сайтом, запись с данными подставного лица.	B	Требуется средняя квалификация. Источник действия может быть и не вычислен (особенно в случае внешнего взлома)	B	Потеря автомобиля (ей).	B
T5	Взлом сайта. Например, для того, чтобы получить права администратора.	C	Требуется средняя квалификация. Вычисление злоумышленника, как правило, затруднительно.	B	Потеря автомобиля. В случае, если злоумышленнику удастся внести соответствующую запись в базе данных.	B
T6	Проведение DDoS-атаки	B	Требуется низкая квалификация. Финансовые затраты минимальны (200 USD за 24 часа атаки по данным из открытых источников).	C	На профильных сайтах может появиться негативная информация, что акция не проводится из-за атаки.	B
T7	Регистрация купонов в большом количестве.	B	Требуется низкая квалификация. Купоны легко насобирать (например, сняв их с упаковок в магазинах)	B	Потеря автомобиля.	B

Еще раз обратим ваше внимание на то, что в случае существующей системы, зачастую необходимо в ходе оценки рисков учитывать наличие уязвимостей и эффективность внедренных контролей. Наверное, никто не будет спорить, что вероятность угона автомобиля возрастает в случае, если мы забываем ключи в системе зажигания. В тоже время оставленная фуражка сотрудника правоохранительных органов может сработать, как «отпугивающий» (deterrent) контроль и снизить риск угона.

Шаг 4. Ранжирование рисков

После проведенной оценки рисков мы сразу можем их ранжировать по значениям, и определять, какому риску уделить внимание в первую очередь, а какому - в последнюю. В нашем случае сначала будут высокие риски, связанные с угроза-

N	Угроза	Обработка риска	Остаточный риск
T1	Внесение логической закладки	**Минимизация:** • Разделение сред. Разработчики создают систему в своей «песочнице». В продуктивную среду коды приложений выкладываются администратором компании-организатора акции. • Анализ исходного кода перед переносом в продуктивную среду.	H
T2	Ошибки программирования, ведущие к уязвимостям системы	**Минимизация:** • Анализ исходного кода перед переносом в продуктивную среду. • Проверка защищенности системы перед вводом в эксплуатацию: сканирование, тестирование на проникновение.	H
T3	Перехват и анализ трафика сервера акции с целью подсчета регистраций и регистрации в нужный момент «своего» купона	**Минимизация:** • Использование шифрования трафика • Выравнивание обхемов. передаваемых данных в ходе успешных и неуспешных регистраций.	H
T4	Внесение в таблицу базы данных, используемых сайтом, запись с данными подставного лица.	**Минимизация:** • Использование шифрования с открытым ключом для внесения данных участника акции. Закрытый ключ хранится у менеджера информационной безопасности до окончания акции.	H
T5	Взлом сайта. Например, для того, чтобы получить права администратора.	**Минимизация:** • Установка всех критичных обновлений безопасности • Настройка системы в соответствии с принятыми в компании внутренними стандартами безопасности • Проверка защищенности системы перед вводом в эксплуатацию: сканирование, тестирование на проникновение	H
T6	Проведение DDoS-атаки	**Передача:** • Сервер системы размещаем в датацентре провайдера. В соглашении с провайдером зафиксированы гарантии защиты ресурсов от DDoS-атак. Провайдер продемонстрировал нам, что соотвествующие меры защиты от DDoS-атак внедрены и риск успешной атаки минимален.	H
T7	Регистрация купонов в большом количестве.	**Минимизация:** • Введение ограничения: 5 купонов на один IP-адрес с последующей блокировкой на 30 минут	H

ми T1-T5 и T7, а затем один средний риск - T6.

Это последний шаг нашей методики оценки рисков, но не последний во всем процессе управления рисками.

Обработка рисков

После того, как мы оценили риски информационной безопасности, мы определяем варианты их обработки.

Выбор возможных действий с риском, к счастью, невелик: мы можем минимизировать риск, внедрив контрмеру(ы), передать его (страхование, аутсорсинг) , избежать, изменив процесс или принять. Чаще всего мы минимизируем риски, а затем принимаем остаточные риски (residual risks).

В нашем случае, мы также решаем минимизировать большинство из них, внедрив соответствующие контроли и один передать внешнему датацентру.

Необходимо отметить, что при внедрении системы менеджмента информационной безопасности, меры выбираются из каталога, приведенного в приложении А к стандарту ISO 27001.

Быстрые «победы» (quick wins)

Зачастую, имеет смысл оценить необходимые для внедрения того или иного контроля ресурсы: финансовые, временные, людские. Наличие таких оценок позволит сделать две вещи: 1) выбрать наиболее экономически целесообразное решение проблемы 2) определить приоритеты по внедрению мер, так как имеет смысл в первую очередь минимизировать высокие риски с помощью недорогих мер (быстрые «победы»).

Остаточные риски должны быть осознанно приняты организацией (в лице владельца рисков).

Цикл PDCA и управление рисками

Проведенная оценка рисков, выбор способов обработки рисков являются составляющей частью этапа «планирования» (Plan) цикла PDCA. Также на данном этапе формируется план внедрения мер с указанием сроков и ответственных лиц. На этапе «исполнения» (Do) данный план выполняется, на этапе «проверки» (Check) проверяется, что принятые меры работают, как следует, а на этапе «действия» (Act), выявленные недостатки исправляются.

Управление рисками и мотивация персонала

Мы с вами понимаем, что наличие хорошо продуманных и формализованных процессов еще не является гарантией успешного функционирования системы менеджмента. Процессы работают тогда, когда работают люди, а люди работают, когда есть мотивация. В области управления рисками работающей практикой является ежегодная подготовка списков наиболее серьезных бизнес-рисков (например, ТОП 20 рисков компании). За каждым риском, закрепляется владелец (обычно это человек «с полномочиями», топ-менеджер), который координирует деятельность по снижению данного риска в течение года. Если один риск повторно оказывается в следующем рейтинге ТОП 20, работа топ-менеджера по данной задаче признается неэффективной и он лишается части своей ежегодной премии.

Магическая формула ALE

Для успешной сдачи экзамена CISSP необходимо помнить следующую формулу:

$$ALE = ARO * SLE,$$

где ALE (annualized loss expectancy) - ожидаемые потери в год, ARO (annual rate of occurrence) – частота возникновения инцидента течение года и SLE (single loss expectancy) – размер потерь в случае одного инцидента.

В определенных, случаях данная формула может использоваться для количественной оценки рисков информационной безопасности.

Например, у нас есть с вами интернет-магазин. Рассмотрим риск его недоступности. Так как мы работаем на конкурентном рынке, в случае недоступности нашего веб-ресурса в течение дня наши клиенты несут свои деньги в магазины конкурентов, и мы теряем прибыль за день (пусть средняя ежеднвная прибыль будет равна 100 000 рублей). У нас с вами есть статистика, что среднем, наш магазин так «выключается» два раза год. Соответственно, можем вычислить ALE:

ALE = 2 * 100 000 = 200 000.

Насколько научной должна быть методика оценки рисков?

При проведении оценки рисков информационной безопасности необходимо помнить, что оценка рисков является составляющей процесса управления рисками, в который вовлечены специалисты различного уровня в нашей организации: от рядового сотрудника до генерального директора. Соответсвенно, применяемая методика должна быть понятна всем участникам процесса. В научной среде все поймут многоэтажные формулы, в среде коммерсантов - цифры потерь, а для большинства будет достаточно цветового обозначения в Excel: красный – высокий, желтый средний, а зеленый – низкий риск.

Заключение

В двух последних статьях мы рассмотрели систему менеджмента информационной безопасности и такую ее ключевую составляющую, как оценка и управление рисками ИБ [1, 2]. Понимание вопросов менеджмента информационной безопасности на уровне основных концепций облегчит сдачу

экзамена для получения статуса CISSP, так как экзамен все больше становится ориентированным на менеджеров ИБ. Для более глубокого погружения в вопросы управления ИБ рекомендуем читателям изучить стандарт ISO 27001:2013.

В следующей статье мы продолжим тему управления ИБ, но перейдем со стратегического уровня на операционный и рассмотрим темы домена «Операционная деятельность по обеспечению информационной безопасности» (security operations). Мы детально рассмотрим такие ключевые процессы информационной безопасности, как управление доступом, управление изменениями и другие [4-7].

Литература

1. Дорофеев А.В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68.
2. Дорофеев А.В. Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1(2). С.67-73.
3. Марков А.С., Цирлов В.Л. Управление рисками - нормативный вакуум информационной безопасности//Открытые системы. СУБД. 2007. № 8. С. 63-67.
4. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012. 968 p.
5. Michael E.Whitman, Herbert J.Mattord. Management of Information Security, Fourth Edition – Cencage Learning, 2014. 566 p.
6. Douglas J. Landoll. The security risk assessment handbook, Second Edition. – CRC Press, 2011. 474 p.
7. Mark Sherling. Practical Risk Management for the CIO. – CRC Press, 2011. 385 p.

References

1. Dorofeyev A.V. Status CISSP: kak poluchit i ne poteryat? Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 65-68.
2. Dorofeyev A.V., Markov A.S. Menedzhment informacionnoj bezopasnosti: osnovnye koncepcii // Voprosy kiberbezopasnosti, 2014, No 1(2). pp. 67-73.
3. Markov A.S., Tsirlov V.L. Upravleniye riskami - normativnyy vakuum informatsionnoy bezopasnosti, Otkrytyye sistemy. SUBD, 2007, No 8, pp. 63-67.
4. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012, 968 p.
5. Michael E.Whitman, Herbert J.Mattord. Management of Information Security, Fourth Edition - Cencage Learning, 2014, 566 p.
6. Douglas J. Landoll. The security risk assessment handbook, Second Edition. – CRC Press, 2011. 474 p.
7. Mark Sherling. Practical Risk Management for the CIO. – CRC Press, 2011. 385 p.