Методика оценки рисков на основе тестирования системы информационной безопасности

С. Е. Голиков

***Аннотация*— Цифровизация экономики сопряжена с ростом угроз безопасности личности, общества и государства в информационной сфере. Оценка рисков является частью комплексного подхода к кибербезопасности и требованием большинства ИТ-стандартов. Использование комплексного подхода в области кибербезопасности позволяет рассматривать все элементы, являющиеся частями кибербезопасности, в качестве сложной, взаимосвязанной системы. Конечной целью данного подхода к кибербезопасности является организация непрерывного процесса защиты от любых физических, программно-аппаратных, сетевых и человеческих воздействий на целевую систему. Интеграция различных уровней и средств защиты обеспечивает более полное понимание уязвимостей и более комплексную защиту от различных угроз. Управление информационной безопасностью (далее-ИБ) является дочерним процессом более широкого процесса управления рисками: если организация после анализа и оценки всех своих бизнес-рисков делает вывод об актуальности рисков ИБ, то информационная безопасность становится средством минимизации некоторых из них. В данной работе предлагается использовать тестирование на проникновение в качестве способа оценки рисков, приведена сравнительная характеристика различных подходов к тестированию для оценки рисковых событий, описаны типы тестирования и их риски, показаны преимущества и недостатки, даны рекомендации по проведению тестирования, использование которых позволяет получить наиболее объективный результат.**

***Ключевые слова*— риски, оценка рисков, тестирование на проникновение, управление рисками в кибербезопасности.**

I. Введение

Оценка рисков является частью комплексного подхода к кибербезопасности и требованием большинства ИТ-стандартов. Использование комплексного подхода в области кибербезопасности позволяет рассматривать все элементы, являющиеся частями кибербезопасности, в качестве сложной, взаимосвязанной системы. Конечной целью данного подхода к кибербезопасности является организация непрерывного процесса защиты от любых физических, программно-аппаратных, сетевых и человеческих воздействий на целевую систему [1]. Интеграция различных уровней и средств защиты обеспечивает более полное понимание уязвимостей и более комплексную защиту от различных угроз.

Тестирование безопасности является одним из наиболее распространенных и часто необходимых способов оценки рисков кибербезопасности, которое помогает выявлять, оценивать и расставлять приоритеты рисков. В процессе проведения тестирования специалист по тестированию защищенности пытается найти те уязвимости, которые легче всего использовать, применяя их с целью получения доступа к нужной информации [2].

Целью данной работы является рассмотрение основных типов тестирования на проникновение с точки зрения оценки рисков, определение достоинств и недостатков использования того или иного метода, влияющих на эффективность данной оценки.

II. Описание стандартной процедуры оценки рисков кибербезопасности

Процесс оценки рисков включает в себя несколько этапов:

1) выявление уязвимостей, угроз и рисков, влияющих на уровень защищенности конкретной организации;
2) оценка вероятности реализации того или иного рискового события;
3) определения приоритетов «смягчения» последствий от их реализации в зависимости от степени риска и вероятности возникновения.

Рекомендации по оценке рисков содержатся в ГОСТ ИСО/МЭК 27005-2010 [3], ГОСТ 13335-1 [4], NIST SP 800-30 [5]. Для расчета риска рекомендуется использование формулы (1):

$$\boldsymbol{R = P_T * P_I * W} \quad (1)$$

где, R – величина риска, P_T – вероятность реализации угрозы T, P_I - вероятность воздействия угрозы на актив I, W – стоимость последствий.

На рисунке 1 показан процесс управления рисками в соответствии с NIST SP 800-39 [6].

Статья получена 02 сентября 2021.

С. Е. Голиков — ФГАОУ ВО «Севастопольский государственный университет (e-mail: kcl@mail.ru).

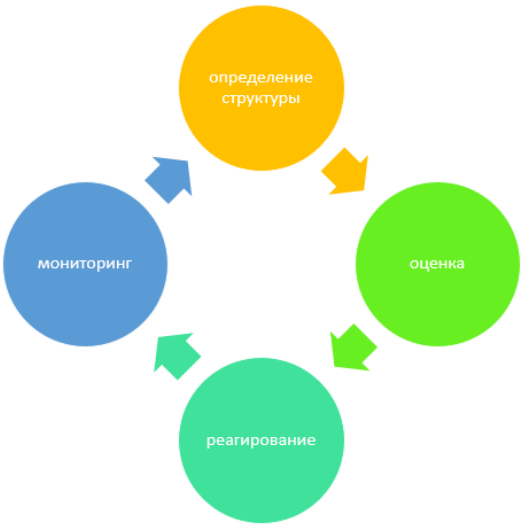

Рисунок 1- Управление рисками в соответствии с NIST800-39

Как видно из рисунка 1, оценке рисков предшествует определение контекста рисков, реагирование на риски и их мониторинг.

Оценка рисков и угроз представляет собой непрерывный процесс, помогающий оценить средства защиты, обнаружить проблемные области и оценить их влияние с целью повышения общей безопасности.

Причинами оценки рисков и угроз являются:

1) предотвращение взломов защиты, утечек и потерь данных. Периодическая инвентаризация защиты и управления кибербезопасностью позволяет обнаруживать и устранять имеющиеся уязвимости;
2) определение уровня защищенности сети. Независимая оценка рисков обеспечивает объективное изучение средств контроля безопасности сети. Она помогает обновить знания о защищенной среде, особенно после таких значительных изменений, как развертывание нового программного обеспечения, установка нового оборудования или переезд в новое место;
3) улучшение процесса принятия решений. Определение влияния выявленных рисков необходимо для планирования бюджета, расставления приоритетов и пр.;
4) сокращение расходов на безопасность. Несмотря на то, что оценка представляет собой достаточно трудоемкую и дорогостоящую процедуру, в будущем она поможет уберечься от более серьезных потерь, предотвратив утечки данных, взломы, нарушения требований действующего законодательства;
5) обеспечение соответствия требованиям регуляторов. Управление рисками является частью многих законов и нормативных актов, несоблюдение которых может привести к значительным финансовым штрафам.

Процедура и инструменты оценки рисков являются уникальными для каждой организации. Однако, в любом случае должны быть выполнены этапы, показанные на рисунке 2.

Рисунок 2 – Этапы управления рисками

Первый этап – определение того, что необходимо защищать. Результатом данной процедуры является список всех данных и ресурсов, которые подлежат защите. Как правило, в данный список входят:

1) персональные данные клиентов и сотрудников;
2) финансовые данные;
3) объекты критической инфраструктуры;
4) конфиденциальные данные, коммерческая тайна и пр.

Второй этап – выявление уязвимостей. На данном этапе, как правило, используются программно-аппаратные средства, позволяющие автоматизировать процесс выявления проблем в системе безопасности на основе известных недостатков программного и аппаратного обеспечения. Результатом является список уязвимостей.

Третий этап – определение угроз и оценка рисков. На данном этапе проводятся:

1) анализ обнаруженных уязвимостей;
2) проработка возможных вариантов использования предыдущего шага;
3) оценка вероятности возникновения рисков;
4) оценка потенциальных последствий выявленных рисков.

Результатом оценки рисков является перечень выявленных рисков, которые ранжируются по степени их серьезности и потенциальному влиянию на деятельность организации. Данный список является основой для планирования и проведения мероприятий по снижению рисков, определения приоритетов, исправления «брешей» в системе безопасности, внедрения новых средств защиты и контроля.

III. Сравнение подходов к тестированию кибербезопасности для оценки рисков

На рисунке 3 показаны три основных подхода к тестированию средств обеспечения безопасности, которые являются наиболее популярными:

1) пен-тестирование;
2) тестирование «красной командой»;
3) тестирование на основе оценки рисков.

Рисунок 3 – Подходы к тестированию кибербезопасности

Пен-тестирование имитирует атаку на системы и приложения организации с использованием широкого спектра ручных инструментов и автоматизированных методов. В ходе процесса тестирования определяются возможные «бреши» в обороне и оценивается потенциальных ущерб, который они могут нанести. Пен-тест также может включать сканирование уязвимостей. Основной целью данного вида тестирования является определение и оценка всех угроз и рисков кибербезопасности для организации.

Тестирование «красной командой» имеет много общего с пен-тестингом. Данный подход также имитирует атаку на защищенную среду, но, в данном случае атака является более продуманной, контролируемой и целенаправленной. Вместо перебора

всех уязвимостей, красная команда выбирает типы данных, которые она хочет получить, составляет список уязвимостей и потенциальных «дыр» в защите, а также действий, которые необходимо предпринять для имитации «сложной постоянной угрозы» (apt-атаки).

Тестирование на основе рисков – вид тестирования, в котором приоритеты действий определяются на основе обнаруженных угроз и рисков. Тестировщики и эксперты по безопасности согласовывают потенциальные риски и оценивают их по уровню критичности. Данный вид тестирования целесообразно применять тогда, когда имеются серьезные временные ограничения, либо необходимо срочно провести оценку рисков с целью улучшения безопасности.

В таблице 1 приведена сравнительная характеристика вышеописанных подходов с точки зрения оценки рисков.

Таблица 1 - Сравнительная характеристика эффективности методов тестирования по отношению к оценке рисков

	Пент-тестинг	**Тестирование «красной командой»**	**Тестирование на основе рисков**
Цель	Комплексная оценка рисков и угроз	Оценка рисков по конкретному направлению	Определение наиболее незащищенных направлений
Характеристики	периодически; после изменения конфигурации системы	Глубокое исследование конкретных уязвимостей и угроз	Время для оценки безопасности ограничено; срочное тестирование и исправление
Участник	Группа внутренней безопасности, внешний эксперт	Внешний эксперт	Группа внутренней безопасности, внешний эксперт
Инструменты	Автоматизированные и ручные средства тестирования информационной безопасности	Ручные инструменты тестирования; использование методов социальной инженерии и имитация реальных атак	Автоматизированные инструменты тестирования безопасности
Продолжительность	Средняя	Длительная	Короткая
Стоимость	Средняя	Высокая	Низкая
Результат	Полный отчет о выявленных недостатках системы защиты информации, уровень воздействия рисков и величины возможных потерь	Отчет с глубокой оценкой определенной компоненты безопасности или тестируемой среды	Проведение тестирования в ускоренном режиме, возможность быстрого покрытия основных рисков и усиления безопасности

Анализ таблицы 1 показывает, что для оценки рисков именно пен-тест является наиболее сбалансированным методом с точки зрения времени, охвата и полноты результатов. Кроме того, регулярное пен-тестирование является требованием многих руководящих документов, например, Положений Банка России 382-П, 683-П и ГОСТ Р 57580.1-2017 [7].

IV. Типы тестирования на проникновение

Существует три типа тестирования на проникновение:

1) тестирование методом «белого ящика»: команда тестирования обладает полным знанием целевой среды, включая знание архитектуры программного обеспечения и исходного кода. Нет необходимости проводить дополнительные исследования или сканирование уязвимостей, тем самым экономится время для дополнительных мероприятий по тестированию. Тестирование методом "белого ящика" может проводиться собственными специалистами по безопасности или сторонними экспертами. Данный тип тестирования используется, когда необходимо проверить защиту на предмет наличия внутренних угроз безопасности. Тестирование методом «белого ящика» включает DoS-атаки, экспертизу памяти, физическое проникновение, обратное проектирование, размытие и т. д.

2) тестирование методом «черного ящика»: команда тестирования практически ничего не знает о программно-аппаратной инфраструктуре. Поэтому она должны использовать любую общедоступную информацию для того, чтобы получить доступ в систему. Данный вариант пен-тестинга имитирует внешнюю хакерскую атаку. Тестирование методом «черного ящика» занимает много времени, но обеспечивает наиболее объективную оценку уязвимостей и рисков безопасности. Для проведения такого пен-тестинга понадобится сторонняя организация. Внутренние ИТ-специалисты не должны знать, что их тестируют. К методам «белого ящика» добавляются методы имитации атак.

3) тестирование методом «серого ящика»: комбинация тестирования методами "белого ящика" и "черного ящика", в ходе которого команда тестирования получает ограниченные данные о программно-аппаратной инфраструктуре, в которую она должна проникнуть. Например, можно предоставить тестировщикам документацию по используемым приложениям, но без учетных данных доступа или исходного кода. Этот тип тестирования занимает меньше времени по сравнению с тестированием методом «черного ящика», но обеспечивает только частичное покрытие кода по сравнению с тестированием методом «белого ящика». Данный тип тестирования также проводится внешними специалистами.

На рисунке 4 показаны достоинства и недостатки каждого из типов тестирования.

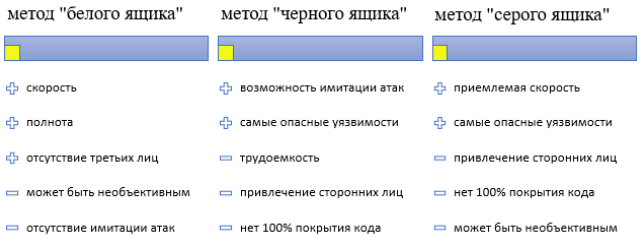

Рисунок 4 – Преимущества и недостатки типов тестирования на проникновение

Процесс проведения тестирования для каждого из типов состоит из трех этапов. На первом этапе, фазе подготовки к атаке производится изучение программно-аппаратной инфраструктуры, периметра сети, сканирование портов, исследование уязвимостей и подбор эксплойтов, выбор инструментов проникновения и пр. При тестировании методом «белого ящика» данный этап включает также сбор целевой информации об организации и ее сотрудниках.

На втором этапе, этапе атаки производится попытка компрометации цели: нарушение защитного периметра, получение и/или повышение привилегий, получение доступа к данным, стирание следов взлома.

Последний этап, этап после атаки заключается в оценке потенциального ущерба и составлении отчета о результатах тестирования на проникновение. Отчет завершает раздел оценки рисков, включающий в себя:

1) описание обнаруженных уязвимостей;
2) описание методологии и инструментов, которые использовались во время тестирования;
3) список как использованных, так и потенциальных эксплойтов;
4) анализ рисков;
5) оценка влияния выявленных рисков на бизнес-процессы.

Таким образом, пен-тестинг является отличным методом оценки средств защиты и рисков кибербезопасности. Однако, сам процесс проведения тестирования на проникновение также должен быть рассмотрен с позиции оценки рисков. Проведение тестирования на проникновение неопытным тестировщиком, либо без детально проработанного плана может принести больше вреда, чем пользы.

V. Ключевые риски тестирования на проникновение

К основным рискам пен-тестирования можно отнести:

1) высокую цену ошибки, особенно при тестировании методом «черного ящика». Пен-тестеры работают с конфиденциальной информацией. Неправильно проведенный тест может привести к сбою оборудования, повреждению или уничтожению данных.
2) нереалистические условия проведения тестов, необъективность результатов. Перед началом тестирования необходимо проверить корректность полученных данных, определить приоритеты будущих улучшений. В противном случае, результаты проведенных мероприятий будут ничтожными.
3) Ограничения по времени и объему. Для проведения пен-тестирования необходимо подготовить техническое задание, определить сроки подготовки отчета. Так как информационная инфраструктура работает в рабочем режиме, перечень используемых эксплойтов существенно ограничен, особенно, если процесс организован с участием сторонней организации. В тоже время злоумышленники могут готовиться к атаке сколь угодно длительное время. Поэтому, нельзя полностью полагаться на результаты однократно проведенного теста, особенно в условиях проведения пен-теста в условиях ограниченности по времени.

VI. Использование «лучших практик» для максимизации результатов пен-тестинга

Каждая команда тестировщиков имеет свою уникальную методологию тестирования на проникновение. Ниже приведены рекомендации, использование которых позволит получить наилучший результат:

1. Тестирование на проникновение должна проводить высококвалифицированная сторонняя команда. Привлечение к процессу тестирования только собственного персонала позволяет сэкономить денежные средства и время. Однако, это не гарантирует объективных результатов, вследствие потенциального отсутствия опыта у тестировщиков, невозможности сымитировать реальную атаку.
2. Тестирование должно охватывать как можно больше компонентов программно-информационной инфраструктуры. Любую инфраструктуру следует рассматривать как целостную систему, а не как набор независимых компонентов. Тестирование и защита части системы не гарантирует, что злоумышленники не смогут добраться до непротестированных компонентов. Низкое покрытие инфраструктуры тестами приводит к возникновению ложного чувства защищенности. Частичное тестирование на проникновение имеет смысл проводить для проверки исправлений в системе безопасности отдельных компонент.
3. Отсутствие спешки при подготовке к тестированию. На этапе подготовки важно оценить максимально полно существующие уязвимости, тщательно подготовить сценарий тестирования. Подготовка является достаточно трудоемким процессом, хотя со стороны может казаться, что ничего не происходит. Для тестирования методом «черного ящика» подготовительный этап может занимать до 90% общего времени.
4. Использование общепринятых стандартов проведения пен-тестирования. Каждая тестируемая среда требует уникального подхода. Тем не менее, существуют общепризнанные стандарты тестирования на проникновение. К ним относятся:
   а) PTES (Penetration Testing Execution Standard) [8];
   б) OWASP Web Application Penetration Checklist [9];
   в) PCI Data Security Standard (PCI DSS) [10];
   г) A guide for running an effective Penetration Testing programme [11].
5. Неизменность программно-аппаратной среды. Пен-тестинг выявляет угрозы и риски в определенном программно-аппаратном контексте. Изменение параметров функционирования автоматизированных систем или развертывание нового программного обеспечения может существенно повлиять на результат. Любые изменения лучше завершить до начала тестирования, чтобы включить новые компоненты среды в процесс тестирования.

6. Проверка целостности мер безопасности и данных после проведения процедуры тестирования. После проведения тестирования на проникновение необходимо тщательно проверить как команда тестирования очистила следы своего пребывания: закрыть созданные бэкдоры, удалить эксплойты и временные файлы, вернуть измененные настройки в первоначальный вид, удалить учетные записи тестировщиков.
7. Использование полученных рекомендаций на практике. Как правило, команда тестирования прописывает в отчетах рекомендации и предложения по устранению рисков. Если тестирование проводится редко или включает в себя большой объем задач, оно, вероятно, выявит множество проблем. Действия по их устранению потребуют значительного количества времени и денежных средств. Для сокращения расходов можно устранить только самые критические проблемы и уязвимости.

VII. Заключение

Оценка рисков является сложной, но жизненно важной частью процесса управления рисками. Она необходима для определения, оценки и приоритезации рисковых событий. Существуют несколько методов оценки рисков, включая тестирование на проникновение, тестирование «красной командой» и тестирование, основанное на оценке рисков. Среди вышеперечисленных методов только тестирование на проникновение позволяет провести комплексную оценку средств защиты и контроля безопасности, включая полноценную имитацию реальной атаки на защищенную среду.

Полученные результаты пен-тестинга можно использовать для:
а) оценки текущего состояния средств защиты и контроля безопасности;
б) оценки механизмов реагирования на инциденты информационной безопасности;
в) определения размеров бюджета на кибербезопасность;
г) определения приоритетов в сфере улучшения информационной безопасности;
д) корректировки и принятия дополнительных мер по усилению информационной безопасности;
е) принятия мер по смягчению последствий инцидентов информационной безопасности.

Таким образом, пен-тестинг является отличным методом оценки средств защиты и рисков кибербезопасности.

Библиография

[1] Holistic security. Доступно по адресу: https://whatis.techtarget.com/definition/holistic-security
[2] Профессиональное тестирование на проникновение: удел настоящих гиков-фанатов командной строки или уже нет? Доступно по адресу: https://habr.com/ru/company/npoechelon/blog/337776/
[3] ГОСТ Р ИСО/МЭК 27005-2010. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Доступно по адресу: https://docs.cntd.ru/document/1200084141
[4] Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Доступно по адресу: https://docs.cntd.ru/document/1200048398
[5] SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. Доступно по адресу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[6] Managing Information Security Risk. Organization, Mission, and Information System View. Доступно по адресу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
[7] УЦСБ. Пентесты для финансовых организаций. Доступно по адресу: https://www.ussc.ru/upload/iblock/a00/a005fa7faa6de6c05de8f0fb3b673eca.pdf
[8] PTES. Доступно по адресу: http://www.pentest-standard.org/index.php?title=Main_Page&action=edit
[9] OWASP Web Application Penetration Checklist. Доступно по адресу:https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Web_Application_Penetration_Checklist_v1_1.pdf
[10] PCI Data Security Standard (PCI DSS). Доступно по адресу: https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf
[11] A guide for running an effective Penetration Testing programme. Доступно по адресу: https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf

Risk assessment methodology based on penetration testing

S.E. Golikov

***Abstract*— The digitalization of the economy is associated with an increase in threats to the security of individuals, society and the state in the information sphere.**

Risk assessment is part of a comprehensive approach to cybersecurity and a requirement of most IT standards. The use of an integrated approach in the field of cybersecurity allows us to consider all the elements that are parts of cybersecurity as a complex, interconnected system.

The ultimate goal of this approach to cybersecurity is to organize a continuous process of protection against any physical, software, hardware, network and human influences on the target system. The integration of various layers and means of protection provides a more complete understanding of vulnerabilities and more comprehensive protection against various threats.

Information security management is a subsidiary process of a broader risk management process: if an organization, after analyzing and evaluating all its business risks, makes a conclusion about the relevance of information security risks, then information security becomes a means of minimizing some of them.

In this paper, it is proposed to use penetration testing as a method of risk assessment, a comparative characteristic of various approaches to testing for assessing risk events is given, types of testing and assessment of their risks are described, advantages and disadvantages are shown, recommendations for testing are given, the use of which allows you to get the most objective result.

Keywords-risks, risk assessment, penetration testing, risk management in cybersecurity.

***Keywords:* risk assessment, penetration testing, risk management in cybersecurity.**

REFERENCES

[1] Holistic security. Dostupno po adresu: https://whatis.techtarget.com/definition/holistic-security

[2] Professionalnoe testirovanie na proniknovenie: udel gikov-fanatov komandnoj stroke ili uzhe net? Dostupno po adresu: https://habr.com/ru/company/npoechelon/blog/337776/

[3] GOST R ISO/MEK 27005-2010. Metody I sredstva obespechenija bezopasnosti. Menedjment riska informacionnoj bezopasnosti. Dostupno po adresu: https://docs.cntd.ru/document/1200084141

[4] Metody I sredstva obespechenija bezopasnosti. Chast 1. Konzepzija I modeli menedzhmenta bezopasnosti informacionnych I telekommunikacionnych technologij. Dostupno po adresu: https://docs.cntd.ru/document/1200048398

[5] SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. Dostupno po adresu: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[6] Managing Information Security Risk. Organization, Mission, and Information System View. Dostupno po adresu: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[7] UCSB. Pentesty dlja finansovych organizacij. Dostupno po adresu: https://www.ussc.ru/upload/iblock/a00/a005fa7faa6de6c05de8f0fb3b673eca.pdf

[8] PTES. Dostupno po adresu: http://www.pentest-standard.org/index.php?title=Main_Page&action=edit

[9] OWASP Web Application Penetration Checklist. Dostupno po adresu:https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Web_Application_Penetration_Checklist_v1_1.pdf

[10] PCI Data Security Standard (PCI DSS). Dostupno po adresu: https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

[11] A guide for running an effective Penetration Testing programme. Dostupno po adresu: https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf