МЕТОДИКА АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

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

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

Аннотация: *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*.

METHODS OF AUDIT OF INFORMATION SECURITY IN MODERN CONDITIONS

Egorov M.A.

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

Abstract: *nowadays information security audit allows to conduct and provide a complete and most objective assessment of the security of information systems, to identify the presence of problems and to develop a suitable and most effective program for the building an information security system of the organization. As part of the information security audit or as part of a separate process, a penetration test can be conducted to verify the ability of the company's information systems 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.*

УДК 007.51

Предпосылки разработки методики аудита информационной безопасности:

- Постоянное развитие технологий и средств атак на информационную систему;
- Зацикленность аудита информационной безопасности на защищенности информационной системы
- Зацикленности аудита информационной безопасности на состоянии информационной системы
- Закрытие глаз и отсутствие проверки способности самой системы к нейтрализации угроз
- Отрицание такого фактора как персонал в ходе аудита информационной безопасности

Анализируя и изучая информацию выше, было выявлено, что аудит информационной безопасности почти не проводит такой анализ безопасности, как анализ «способности системы нейтрализовать угрозы и избегать опасность. Поэтому мною было решено разработать данную методологию.

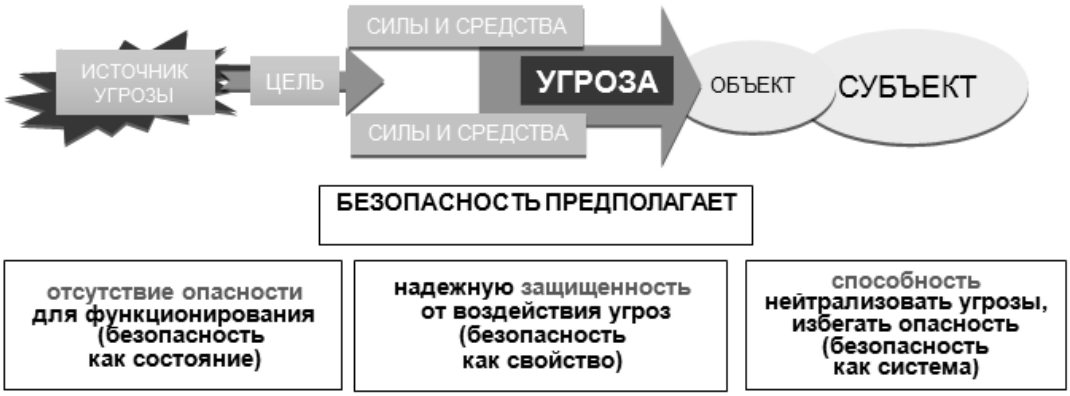

Рис. 1. Модель угрозы и ориентиры безопасности

Для построения методологии было проанализировано существующие методы проведения аудита информационной технологии, изучил критерии, которые они рассматривают, благодаря посещению конференции по практической кибербезопасности “Positive Hack Days 2019” от компании Positive Technology , мне удалось познакомиться с многими компаниями, которые имеют в наличии услуги по аудиту информационной безопасности, обсудить с ними мою методологию и прийти к выводу, что на рынке отсутствует аудит информационных систем, направленный на определение уровня способности систем нейтрализовать угрозы, которым она может быть подвержена либо подвергается в режиме реального времени [1].

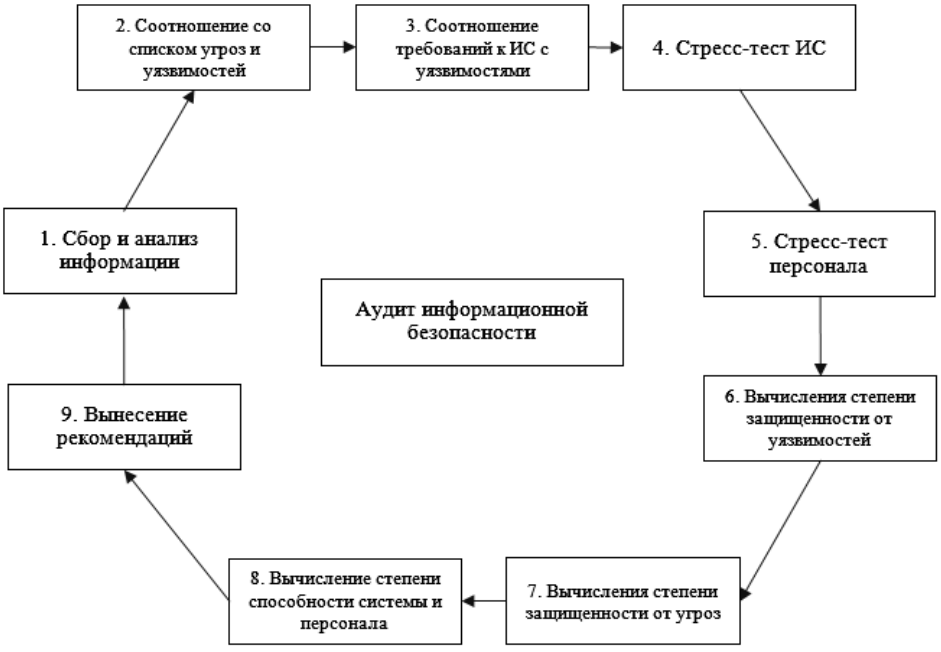

Рис. 2. Процесс аудита информационной безопасности в современных условиях

Этап 1 - Сбор информации

Данный этап является основополагающим для начала аудита информационной безопасности систем дистанционного банковского обслуживания, так как на нем собирается основная информация, которая касается деятельности организации, её политик, регламентов, приказов по вопросам обеспечения информационной безопасности информационных систем, а также информация о аппаратном и программном обеспечении информационных систем: серверов, компьютеров, - задействованных в осуществлении процесса взаимодействия клиентов и сотрудников компании, топологии глобальных и локальных вычислительных сетей.

Важным пунктом являются наличие, актуальность и полнота данной информации, любое отсутствие является недостатком в организации, и должно быть учтено специалистом, осуществляющим аудит, так как каждый процесс должен быть полностью описан и документирован.

Этап 2 - Соотношение со списком угроз и уязвимостей

На данном этапе эксперты должны категорировать полученную ими информацию об информационной системе, её аппаратно-программном обеспечении, средствах защиты информации и рассмотреть возможные потенциальные угрозы и уязвимости, которые могут иметь место в них, на основе CVE - базы данных общеизвестных уязвимостей информационной безопасности и базы данных угроз ФСТЭК.

Этап 3 – Соотношение требований к информационной системе со списком уязвимостей и угроз

На следующем этапе специалист осуществляет поиск эксплойтов которые будут применяться для проверки триггеров системы и систем мониторинга, компилирует их в специально выполняющуюся программу (скрипт), чтобы затем реализовать [2].

Этап 4 – Стресс-тест информационной системы

После осуществления поиска и создания программы для аудита информационной системы, аудитор (высококвалифицированный специалист) осуществляет запуск данной программы, сотрудники компании наблюдают за различными триггерами, которые должны среагировать на каждый эксплойт, действие производится с 3 рубежей – внутри компании, вне компании в качестве злоумышленника и вне компании в качестве клиента банка.

Этап 5 – Стресс-тест персонала

Пока осуществляется тест информационной системы, аудитор осуществляет поверку персонала на общие знания в сфере информационной безопасности, методов противостоять угрозам информационной безопасности путем сбора информации по параметрам инцидентов, а именно: даты и времени создания заявки, количества шагов для его устранения и времени затраченного на это; а также осуществляет анкетирование сотрудников и получение обратной связи по фишинговой проверке, в которую входят методы дезинформирования персонала, выдачи ложной информации за действительность и дискредитирование других сотрудников для проверки их способности противостоять информационно-психологическому воздействию.

Этап 6 – Вычисление уровня защищенности от уязвимостей

После осуществления стресс-тестов аудитор производит качественную оценку уровня защищенности систем на наличие уязвимостей, через которые могут быть реализованы угрозы.

Этап 7 – Вычисление уровня защищенности от угроз

На данном этапе производится оценка защищенности системы и персонала от угроз, которые могут быть реализованы через имеющиеся уязвимости в информационной системе и организации, при этом стоит учитывать тот факт, что уязвимости не могут быть предельным числом, так как каждая система и человек уязвимы в той или иной степени.

Этап 8 - Вычисление степени способности системы и персонала нейтрализовать угрозы

Этот этап является ключевым в данном аудите, так как по ранее перечисленным этапам уже созданы различные методологии и методы оценки. Для осуществления вычисления уровня способности системы и персонала нейтрализовать угрозы необходимо, во-первых, наличие систем, которые предупреждают появление угроз, путем отслеживания нелегитимных изменений в системе или её состоянии, во-вторых, наличие автоматической способности выявления последствий, путем автоматического мониторинга целостности системы, её характеристик, файлов, программ, и обеспечивающие её восстановление, в-третьих, наличие систем по уменьшению ущерба, способных в реальном времени осуществить восстановление копии файлов, поврежденного участка кода, сети, уязвимой части системы и, в-четвертых, наличие систем мониторинга, которые позволяют персоналу, обслуживающему данную систему отслеживать происходящие изменения в системе как во внутреннем периметре, так и во внешнем. Только при наличии подобного обеспечения необходимо использовать полученную информацию о всех событиях, которые происходили в момент стресс-теста ИС и персонала, а также выявить, какое количество событий было нейтрализовано системой и персоналом в сумме, а какое количество событий были не замечены.

Этап 10 – Вынесение рекомендаций

На данном заключительном этапе осуществляется формулирование рекомендаций по повышению уровня способности реагирования на угрозы и их нейтрализации, а также уровня защищенности информационной системы – стадия разработки предложений и документирования полученных результатов.

К рекомендациям по доработки системы можно отнести:

- доработка и донастройка систем, программ и сценариев, направленных на предупреждение угроз, выявление последствий и нейтрализации угроз.

К рекомендациям по повышению уровня квалификации персонала можно отнести:

- Обучение сотрудников вопросам кибербезопасности, назначение;
- Назначение тренингов и тестов;
- Повторное тестирование персонала
- Контроль результативности обучения

Таким образом, была описана методология осуществления аудита информационной безопасности в современных условиях и перечислены основные рекомендации по повышению уровня способности систем и персонала нейтрализовать угрозы информационной безопасности [3].

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.