Лекция 15. Управление рисками кибербезопасности. Карьера специалиста по кибербезопасности

Цель лекции: познакомиться с понятием управление рисками кибербезопасности; и рассмотреть вопросы карьеры специалиста по кибербезопасности.

План лекции:

1. Управление рисками кибербезопасности.
2. Карьера специалиста по кибербезопасности

Управление рисками кибербезопасности

Управление рисками информационной кибербезопасности представляет собой циклический процесс, состоящий из идентификации рисков, оценки опасности и проактивной минимизации тяжести возможных в случае реализации рисков последствий. Данный процесс позволяет выделить уязвимые места в системе защиты, а также оценить затраты на их устранение.

Целью этой деятельности является просчет адекватной защиты активов организации. Для этого необходимо не только построить модель угроз и модель нарушителя, но и провести детализированный анализ возможностей реализации рисков с выработкой мер по их снижению.

Определение.

• **Риск** – это вероятность возможнойнежелательной потери чего-либо приплохом стечении обстоятельств.

• **Риск информационной безопасности** – вероятность возникновения ущербавследствие нарушения целостности,конфиденциальности и доступностиинформационных активов.

Управление рисками позволяет:

1. Определять карту рисков компании.

2. Формировать перечень актуальных угроз информационной безопасности. В Систему включена база данных угроз ФСТЭК, а также имеется возможность дополнения перечня пользователями системы.

3. Формировать перечень уязвимостей, через которые возможна реализация угроз. В систему включены типовые уязвимости, а также имеется возможность дополнения перечня пользователями системы.

4. Формировать перечень мер защиты. В систему включены типовые меры защиты, а также имеется возможность дополнения перечня пользователями системы.

5. Определить область оценки и собрать полную информацию о текущих бизнес-процессах.

6. Сформировать модель угроз и нарушителя для каждого актива компании.

7. Провести комплексную автоматизированную оценку рисков информационной безопасности с привлечением экспертов от различных структурных подразделений.

8. Выработать детальный план обработки рисков, проследить за стадиями его выполнения и результатами применения защитных мер.

9. Провести экспресс-оценку сотрудниками компании собственных бизнес-процессов без привлечения сотрудников подразделения информационной безопасности.

Рисунок 1 Ландшафт киберрисков

В мире существует множество методологий построения процессов управления рисками и первичной оценки рисков.

Coras, CRAMM, PRISM, RiskWatch, OCTAVE – это всего лишь малая часть перечня существующих практических методик. Есть унифицированные методики, есть отраслевые.

- ISO 27005
  - NIST SP 800-30 и 800-66
  - FRAP (Facilitated Risk Analysis Process)
  - OCTAVE (Operationally Critical Threat, Asset, and VulnerabilityEvaluation
  - FAIR (Factor Analysis of Information Risk)
  - AS/NZS 43 60• CRAMM (CCTA Risk Analysis and Management Method)
  - Spanning Tree Analysis

- ENISA
- Harmonized Threat and Risk Assessment Methodology
- РС БР ИББС-2.2

Примеры

Источник угрозы	Использует уязвимость	Возникает угроза
Вирус	Отсутствие антивирусного программного обеспечения	Заражение вирусом
Хакер	Уязвимости в коде Отсутствие системы обнаружения вторжений	Несанкционированный доступ к конфиденциальной информации
Пользователи	Неверно настроенный параметр операционной системы	Неисправность системы

Менеджмент риска

№	Этапы	Действия
1	Планирование	Определение области оценки риска и IRM-группы
2	Анализ и оценка рисков	идентификация и оценка активов идентификация угроз идентификация уязвимостей анализ защитных мер прогнозирование последствий оценка вероятности реализации угрозы измерение уровня риска
3	Обработка рисков	Выбор варианта реагирования на риски: - уход от риска - минимизация риска - перенос риска - принятие риска
4	Реализация плана обработки риска	Проведение мероприятий, направленных на управление рисками (внедрение защитных мер, отказ от деятельности, страхование риска, проведение обучения по повышению осведомленности персонала и партнеров организации во вопросам ИБ и т.д.)
5	Контроль и мониторинг	Регулярная оценка риска и отслеживание влияющих на него факторов

Карьера специалиста по безопасности

ОЦЕНКИ РЫНКА. $232 млрд достигнет объем рынка кибербезопасности к 2022 году со среднегодовым темпом роста в 11% за период с 2017 года.

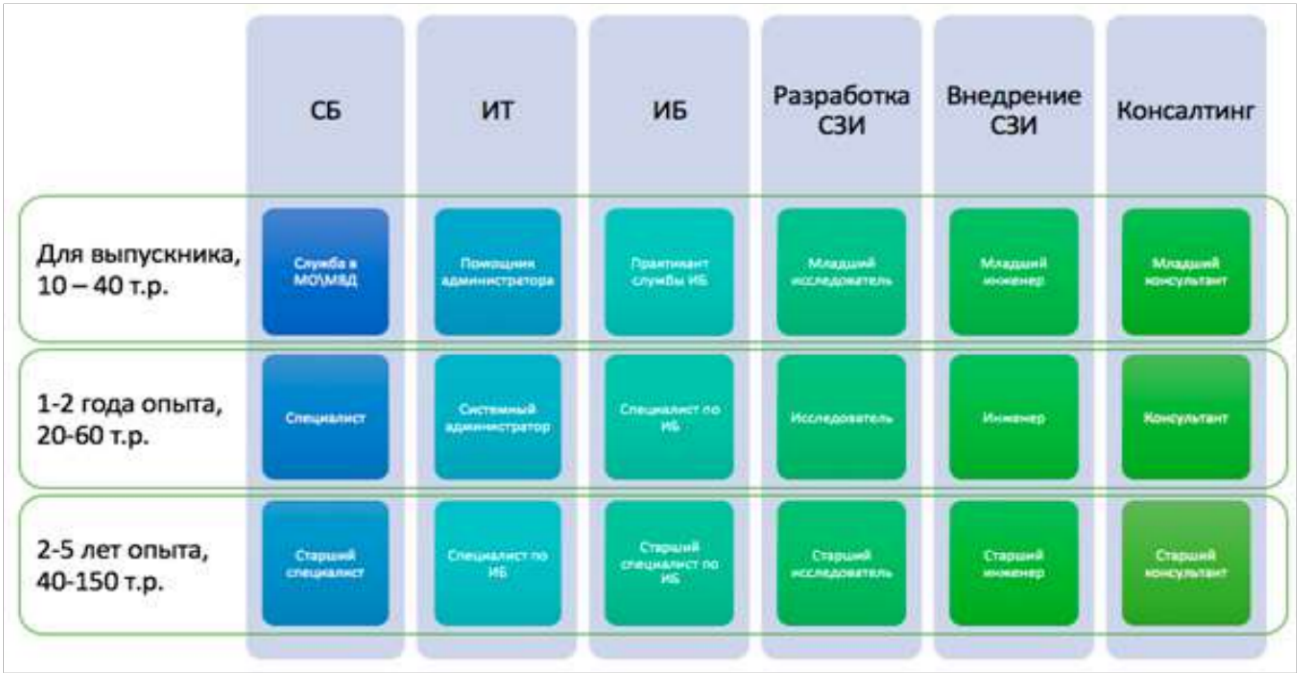

Рисунок 2 Карта карьеры

По данным исследования SuperJob от 2016 года работодатели в целом ценят следующие 9 тематик:

1. знания нормативно-правовой базы, руководящих документов, государственных стандартов в сфере информационной безопасности;
2. знания стандартов шифрования, основных технологий обеспечения информационной безопасности, современных программных и аппаратных средств защиты информации;
3. навыки настройки и конфигурирования современных решений защиты информации (межсетевые экраны, системы обнаружения и предотвращения атак и проч.);
4. опыт проведения аудита информационной безопасности;
5. опыт разработки регламентов и политик безопасности;
6. опыт проведения расследований внешних и внутренних инцидентов в сфере информационной безопасности;
7. сертификаты по информационной безопасности;
8. опыт реализации систем информационной безопасности в крупных корпоративных сетях;
9. опыт проектирования эксклюзивных систем и методов защиты информации.

Практика развития компетенций

- Производственная практика.
- Волонтерство.
- Сертификации по информационной безопасности. Для направления policy ключевые сертификаты CISSP, CISM, CISA, CRISC. Для направления technology сертификаты Microsoft, Cisco, CEH, OSCP.
- Сообщества по информационной безопасности.
- Изучение и конспектирование книг, руководств и курсов.
- Фриланс.
- Изучение английского языка. Без английского языка в сфере кибербезопасности будет сложно достичь сколь-нибудь заметных высот.

Топ-5 популярных профессий в сфере кибербезопасности

1. Анти-фрод аналитик

Востребован в банковской сфере и финтех компаниях. Отвечает за безопасность онлайн-операций с финансами для физических лиц, например, в "онлайн-банке". Устанавливает и отслеживает лимиты на количество покупок по одной банковской карте, на максимальную сумму разовой покупки по одной карте или одним пользователем, количество банковских карт, используемых одним пользователем в определенный период времени. Ведет учет и анализирует историю покупок пользователей для выявления подозрительных операций.

2. Специалист по реверс-инжинирингу или аналитик кода

В задачи специалиста входит детальный разбор программного кода с целью выявить уязвимости программы для кибератак. Специалист должен понимать общие принципы программирования, знать языки, как минимум C++, ASM, Python, знать виды уязвимостей OWASP Top 10, SANS Top-25. После анализа кода и выявления угроз специалист дает рекомендации по защите системы.

3. Разработчик системы защиты информации (СЗИ)

Специалист совмещает в себе знания и навыки разработчика со знанием средств защиты информации. Важны навыки программирования, знание языков CI\CD, облака AWS или MS Azure, фреймворков, антивирусов и DLP-систем. Разрабатывает в компаниях внутреннюю систему защиты информации и отслеживания кибератак.

4. Специалист по форензике или расследованию кибер-преступлений

Чаще всего наемные специалисты, которые расследуют компьютерные или финансовые преступления: взломанные серверы, десктопы, СУБД. Проводят поиск следов взлома, восстанавливают сценарий кибератаки, временную цепочку событий, фиксируют нарушения. Собирают улики и

разоблачают преступные группировки хакеров. Владеют языками программирования, понимают как работают средства защиты и как их обходят хакеры.

5. Пентестер

Специалист, который тестирует систему, проверяет, насколько хорошо защищены данные. Выявляет слабые места, укрепляет защиту данных. Исследует целостность информационной системы. Пентестеров нанимают, обычно, крупные IT и финансовые компании, которые оперируют большими данными. Пентестерам необходимы глубокие знания ОС Windows\Linux, сетей, уязвимостей.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.
2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.
3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.
4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582
5. Carl A. Sunshine. Computer Network Architectures and Protocols. — Springer Science & Business Media, 2013-06-29. — 542 с. — ISBN 978-1-4613-0809-6.