Deloitte.

Управление рисками информационной безопасности

MAKING AN IMPACT THAT MATTERS since 1845

Ведущие вебинара

Владимир Ремыга, CISA, CISSP, CGEIT, CRISK, PRINCE 2

Директор

vremyga@deloitte.com

+7 700 714 5505

Владимир руководит практикой консультационных услуг Deloitte в области ИТ рисков и кибер-безопастноси в Каспийском и Кавказском регионах. Обладая 25 летним опытом, он оказывает консультационные услуги для большого числа коммерческих и не коммерческих организаций и специализируется на услугах в направлении: цифровой трансформации, ИТ архитектуры, управления кибер-рисками, оптимизации ИТ затрат и повышения эффективности.

Содержание

- **Идентификации активов**
- **Определение кибер угроз**
- **Выявление уязвимостей**
- **Анализ рисков ИБ**
- **Управление рисками ИБ**

Модель управления угрозами ИБ

Критичные активы

- Учетные данные
- Конфиденциальная корреспонденция
- Персональные данные
- Рабочие места администраторов и разработчиков
- Базы данных
- Данные платежных карт

Меры защиты

- Network Firewalls
- IP Whitelisting
- Network Isolation/Segmentation
- Segregation of duties
- Data Encryption
- Antimalware
- Least Privilege Access Model
- Hardened Services
- IPS/IDS
- Security Monitoring

exploits

Высокие риски

Уязвимости

- Ошибки в ПО
- Уязвимости в ПО
- Ошибки в инфраструктуре

Угрозы

- Внешние угрозы
- Внутренние угрозы
- Третьи стороны

Идентификации активов

Идентификация информационных активов

С точки зрения бизнеса, информационная безопасность должна быть сбалансирована с ценой защищаемых активов

Информационный актив - информация с реквизитами, позволяющими ее идентифицировать и имеющая ценность для организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Примеры информационных активов:

- Бизнес процессы.
- Данные (электронные, печатные, другие).
- Сотрудники.
- Оборудование (сервера, рабочие станции, другое).
- Программное обеспечение.

Вопросы для анкетирования

1. Какие бизнес процессы выполняет Ваш отдел?
2. Какие ИТ-приложения Вы используете в работе?
3. Какого рода информацию Вы используете в работе? (перечислить все информационные активы: базы данных и файлы данных, системная документация, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки (обслуживания), планы по обеспечению непрерывности функционирования информационного обеспечения, процедуры действий при сбоях, архивированная информация)
4. Откуда, от кого Вы получаете информацию? Каким способом Вы ее получаете?
5. Где хранится используемая Вами информация? На каких носителях (бумажных, электронных), в каких местах (шкафы, сейфы, файловые сервера, компьютеры, ИТ-системы)?
6. У кого есть право доступа к этой информации: подразделения, определенные сотрудники, сторонние организации?
7. Куда Вы передаете информацию? Каким способом?
8. Каким способом происходит утилизация информации?
9. Оцените имеющуюся у Вас информацию по степени конфиденциальности:
   - Коммерческая тайна;
   - Служебная тайна. (данные служебного пользования);
   - Публичная информация.
10. Оцените существенность разглашения данной информации по 5-ти бальной шкале?
11. Если информация должна обладать требованиями защиты от искажения, нарушения доступности, подлинности, неотрекаемости, подотчетности и по контролю использования, адекватности информации и пр. Просим указать эти требования и дать им оценку существенности.

Определение кибер угроз

Источники угроз
Что такое источник угрозы?

Источники угрозы - внешние или внутренние нарушители, третьи лица, силы природы.

Внешние нарушители не являются сотрудниками компании, легитимными пользователями внутренних информационных систем, аутсорсерами, подрядчиками, поставщиками, заказчиками и прочими лицами, связанными юридическими отношениями с рассматриваемой организацией. Такие нарушители не имеют легитимного доступа к объекту защиты - информационному активу.

Внутренними нарушителями могут считаться физические лица - сотрудники и руководители компании, а также юридические лица работающие по контракту. В общем, это все лица, которые имеют внутренний доступ к защищаемому информационному активу. Как правило, внутренние нарушители отличаются некоторым уровнем знания о работе атакуемого актива, имеют или могут сравнительно легко получить к нему доступ, причем зачастую санкционированный и с расширенными полномочиями.

Третьими лицами - еще одной категорией источников угрозы - можно считать органы государственной власти, которые формально не входят в число потенциальных внешних нарушителей, однако последствия от их вмешательства в работу компании могут быть соразмерны с воздействием стихийного бедствия.

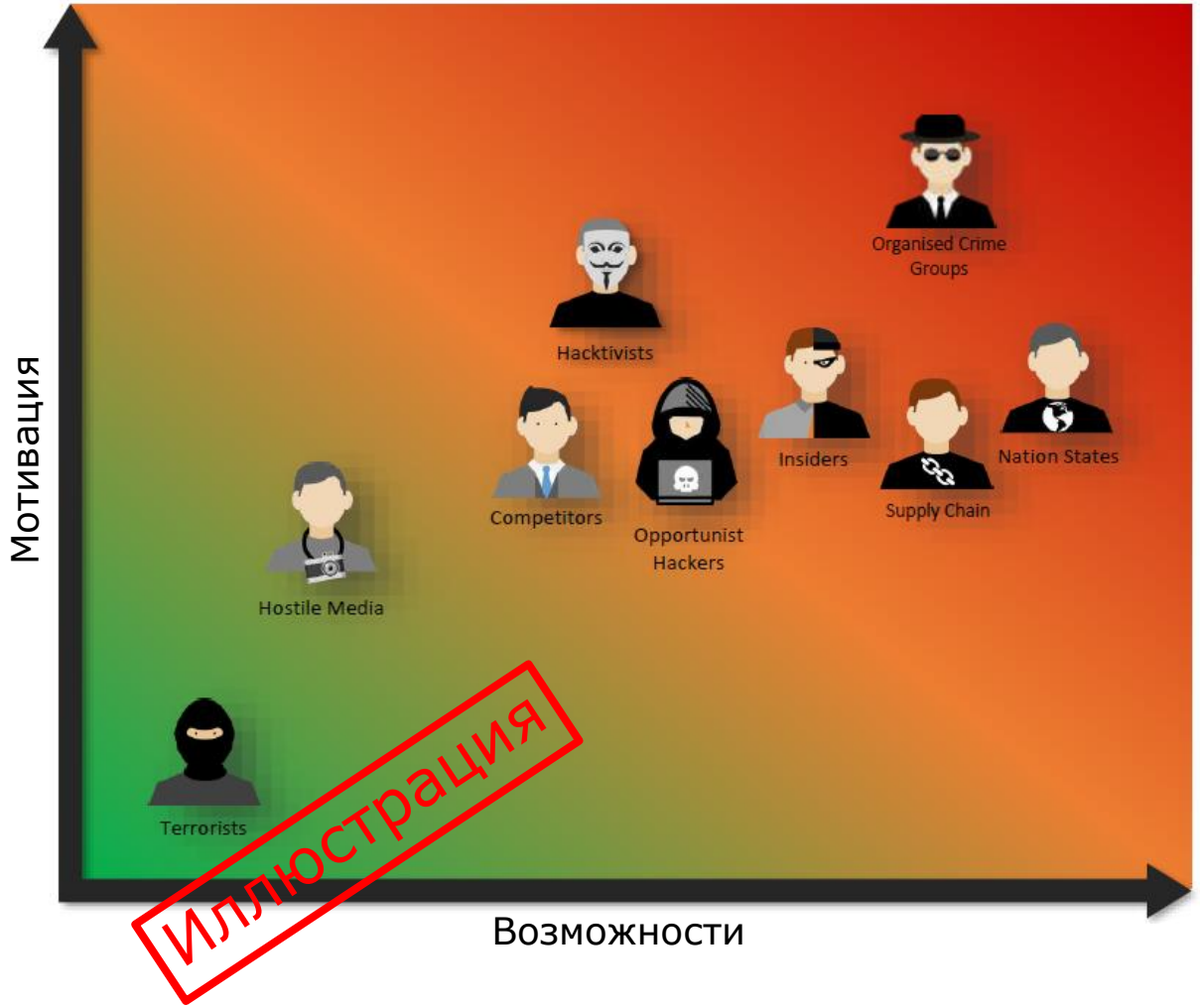
Кибер-преступник, кто он? Как узнать? Попробуйте идентифицировать.

Наши герои:

1. Фрэнк Абигнейл - был приговорен к 12 годам лишения свободы за мошенничество.
2. Ванг Женгянг – 13 лет. Взломал компьютерную систему школы с целью прогуливать уроки. Он также обвинялся в мошенничестве при оплате товара в онлайн магазине, где он изменил стоимость ноутбука с $400 на $0,16.
3. Оуен Вокер - обвинялся в организации международной преступной хакерской группы, во взломе систем, создании бот-сетей. Был освобожден от заключения, так как не достиг совершеннолетия.
4. Кевин Митник - неоднократно совершал преступления, связанные с проникновением в компьютерные сети.
5. Дэвид Кернелл - предъявлено обвинение во взломе электронной почты американского политика Сары Палин.
6. Джозеф МакЭлрой - приговорен к 200 часам общественных работ за проникновение в сеть государственного учреждения США. На момент проникновения ему было 16 лет.
7. Кристина Шечинская – 21 летняя россиянка. Одна из девяти соучастников обвиняемых в хищении 3 миллионов долларов из американских банков при помощи хакерского ПО
8. Саад Ичуафни - разыскивается ФБР за организацию и проведение DDOS - атак.

Источники кибер угроз

Для определения уровня кибер угроз необходимо проанализировать их источники, оценив для каждого из них возможности и мотивацию для атак на Вашу организацию.



Для всех источников угроз с высоким уровнем определяются характерные для каждого из них наиболее вероятные вектора и сценарии атак

Источник	Возможности	Мотивация	Уровень угрозы
Организованные преступные группы	Высокие	Высокая	Высокий
Спец службы	Высокие	Средняя	Высокий
Инсайдеры	Высокие	Средняя	Высокий
Поставщики	Высокие	Средняя	Высокий
Хактивисты	Средняя	Высокая	Высокий
Хакеры одиночки	Средняя	Средняя	Средний
Конкуренты	Средняя	Средняя	Средний
Враждебные СМИ	Низкие	Средняя	Низкий
Террористы	Низкие	Низкая	Очень низкий

Иллюстрация

Источники кибер угроз: Спец службы

Nation States

Возможности — Высокие

Самая ресурсоемкая группа из всех действующих лиц угрозы. Группы спонсируемые государством оказались очень коварными и преобладающим видом угроз в современном мире. Эти группы часто возникают из разведывательных службы (FIS) и как правило, являются из частью. Поддерживаясь каким-нибудь правительством и обладая высоким уровнем технических возможностей и знаний они способны целенаправленно изучать, запускать и поддерживать различные виды атак, в том числе типа APT, против их противников.

Данный источник угроз можно считать весьма эффективными в своих подходах к разведке, доставке и реализации атак. Они также часто остаются незамеченными.

Мотивация — Средняя

Скорее всего, у субъектов государства будет широкий спектр мотивов для нацеливания на банк. Часто они просто хотят приобрести большие источники персональных данных, чтобы профилировать или контролировать финансовую деятельность известных или состоятельных лиц. Там также им может быть интеллектуальная собственность банка, учитывая его амбиции и прогресс на сегодняшний день в регионе, став одним из первым настоящим цифровым банком.
Иностранные державы могут также быть заинтересованы в нарушении или манипулировании стабильностью социального уклада и экономики в Казахстане. Ориентируясь на услуги, предоставляемые финансовыми институтами они могут старятся дестабилизировать работу. С точки зрения всего финансового сектора, это может быть незначительным, однако может являться частью более широкой и долгосрочной кампания по подрыву социального строя и экономики страны в целом.

Вектора и сценарии атак

Так называемые «Продвинутые постоянные угрозы» (APT). Финансируемые государством группы имеют уникальное сочетание ресурсов, технических навыков и времени, которое позволяет им длительное время использовать технически сложные подходы к скрытому получению доступа в хорошо защищенные сети. Воплощением набора инструментов APT, являются атаки «Нулевого дня». Уязвимости в программном обеспечении или сети, которая известна только злоумышленнику, и способна долгое время быть неизвестной. Следует, однако, отметить, что Zero Day требуют значительных ресурсов, и следовательно, их использование, вероятно, будет ограничено для особо важных целей. Более того, как и все другие субъекты киберугроз, спец службы и их доверенные лица достаточно прагматичны в их методологии таргетирования и будут использовать путь наименьшего сопротивления.

Атаки социальной инженерии. В последнее время было отмечено использование социальных медиа платформ, чтобы устанавливать дружеские и доверительные отношения с сотрудниками банка, обладающими доступом к критически важной информации.

Атаки через поставщиков также усиливаются. Учитывая достаточное время и ресурсы, нарушение безопасности организации нацеливание на оборудование или программное обеспечение, предназначенное для использования в организациях до их развертывания (или через последующие обновления, как было в случае с NotPetya).
Похожие угрозы замечены и в отношении системы провайдеров управляемых предоставляющих услуги банку. Есть основания полагать, что все три варианта (аппаратные / программные / доступ человека) все чаще эксплуатируются, что указывает на то, что независимо от существующих механизмов все они еще могут представлять угрозу и должны быть рассмотрены.

Уровень угрозы — **Высокий**

Иллюстрация

Источники кибер угроз: Инсайдер

Возможности

Высокие

Инсайдеры с законным доступом к системам банка и его информации о контрольной среде в сочетании с знанием технологического ландшафта, дает им значительное преимущество для реализации угроз. Более того, это зачастую позволяет им обойти контроли безопасности и избежать своевременного обнаружения деяний.

Есть также основания полагать, что в последние годы Инсайдеры могут рекламировать свою готовность к сотрудничеству с более способными злоумышленниками (источниками угроз) например в криминальных форумах DarkWeb. Тем самым они представляют исключительноую опасность, при которой ключевые элементы управления, такие как привилегированный доступ или безопасное удаленное подключение можно легко скомпрометировать.

Мотивация

Средняя

Мотивация инсайдера (контрактник или мошенника) часто зависит от ряда факторов, такие как: чувства, культура и мышление рабочей силы в целом, а также личная ситуация человека, которая может включать финансовые проблемы / долги, зависимость, азартные игры, злоупотребление наркотиками и т. д. Также очень часто такие источники находятся в поисках быстрой известности / мести работодателю. Какими бы ни были обстоятельства, сила их мотивация будет решающим фактором в определении того, может ли сотрудник переступить моральную т.е. вести себя в соответствии с политиками и стандартами банка или примет решение о порочном пути, который может привести к кибер-атаке, фроду или другим нарушениям.
Мотивация инсайдера также может совпадать с намерением хактивиста или враждебного СМИ, учитывая, что такие субъекты могут угрожать подать заявку на внутреннюю позицию, а затем стремиться совершать гнусные поступки или сотрудничать с другими, более способными цели.

Вектора и сценарии атак

Инсайдеры имеют значительное преимущество в том, что им не нужно проводить начальные шаги к цепи кибер-атаки: их законный доступ к системам позволяет им входить в сеть и системы. Поэтому основные их цели в первую очередь заключаются в следующем:

- повысить уровень привилегированного доступа в сети или информационной системе.
- Двигаться в направлении, чтобы добраться до систем, на которые они нацелены
- Получить доступ и осуществить извлечение информации / данных (если это их цель) без обнаружения.

Съемные носители (например, USB-накопители, портативные жесткие диски и т. Д.) Являются отличным средством для таких мошенников. Они способны внедрить вредоносное ПО в целевую систему, а также осуществить удаление или шифрование данных.

Кроме того, если организации низкий уровень защиты передаваемых данных по каналам связи (например, электронная почта, обмен файлами, облачные платформы и т. д.) кража или подмена данных инсайдером может быть относительно простой задачей для выполнения, при этом без своевременного обнаружения.

Помимо вывода данных / информации, банк также должен рассмотреть Инсайдера как потенциального источника для реализации атак способных нарушить работу операционных систем, используя как технические, так и физические средства, такие как:

- DoS-атака, приобретаемая у третьей стороны (например, Cyber Attack as a Service)
- Отключение критических компонентов системы / сети.

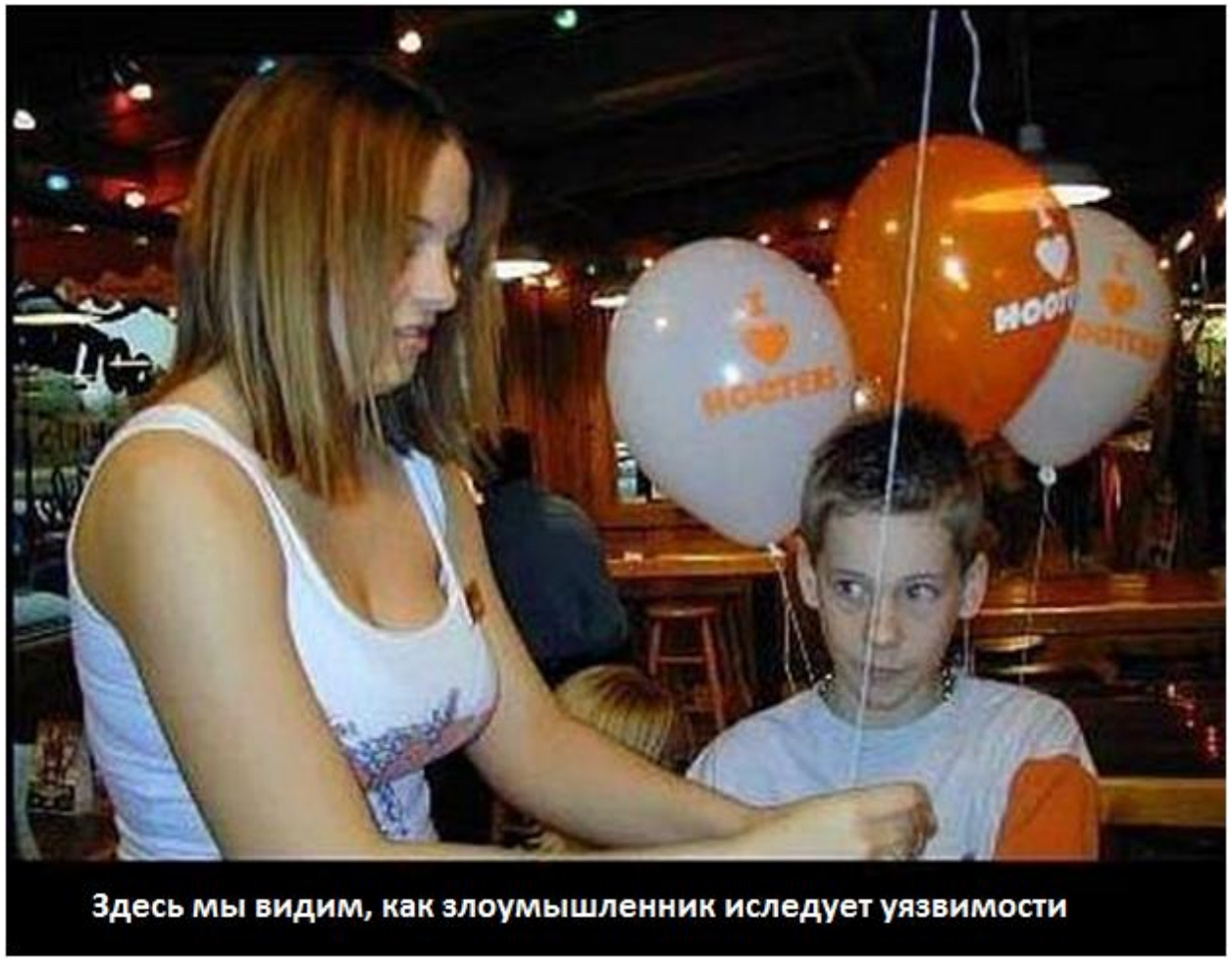
Иллюстрация

Уровень угрозы **Высокий**

Выявление уязвимостей

Выявление уязвимостей

Уязвимость - это недостаток средств защиты информационной системы, который может быть использован для реализации угроз информационной безопасности. Уязвимости информационной системы могут быть порождены как ошибками при создании, внедрении или эксплуатации системы, так и слабостью наложенных защитных средств и примененных мер. Защитные меры традиционно подразделяют на организационные, технические, физические и применяют их к сотрудникам, процессам и технологиям. По целям применяемых мер существует разделение на предупредительные, директивные, превентивные, сдерживающие, корректирующие, восстановительные, расследовательные и компенсирующие меры.



Здесь мы видим, как злоумышленник иследует уязвимости

Выявление уязвимостей

Выявление уязвимостей позволяет получить понимание существующих недостатках в защите систем и процессов обеспечения ИБ организации, а также оценить приоритетность мероприятий, направленных на защиту её критичных активов.

Выявление уязвимостей включает анализ нескольких областей, покрывающих различные области и аспекты деятельности организации.
Каждая область анализируется отдельно и как правило отдельной методологией и видом инструментария.

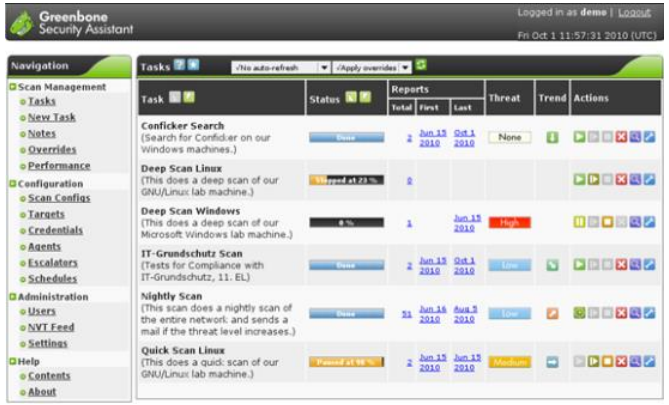
Наиболее распространёнными способами выявления уязвимостей являются:

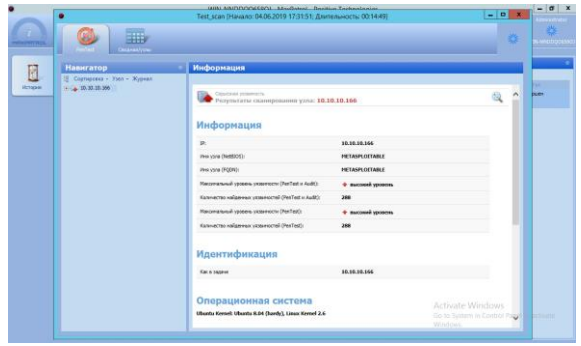
1. Анализ на возможность проникновения (Penetration test).
2. Сервис выявление уязвимостей (Vulnerability Management and Scanning Service)
3. Фишинг как сервис (Phishing as a service)
4. Самостоятельное использование специализированного ПО для выявления уязвимостей программного и аппаратного обеспечения.

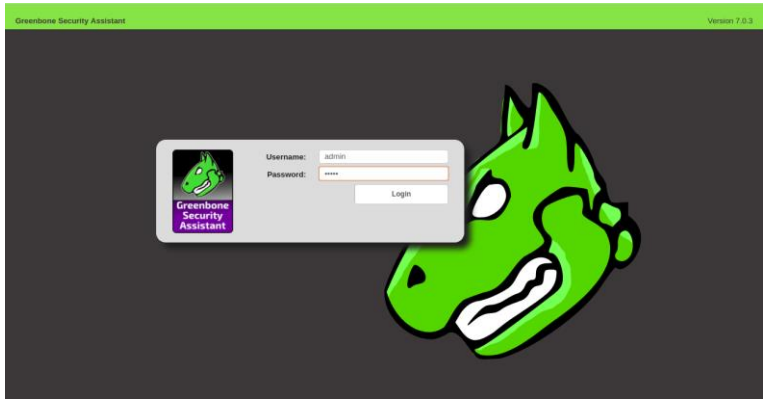
При тестировании каждой области оценивается процесс реагирования на инциденты информационной безопасности и возможности по восстановлению работоспособности, в случае возможной компрометации безопасности ИТ систем.

Инструменты выявления уязвимостей

- OpenVAS.
- Nessus.
- MaxPatrol и т.п.







Глобальные базы уязвимостей

https://www.securityfocus.com

https://www.exploit-db.com/

https://www.cvedetails.com

https://vuldb.com

https://vulners.com

https://www.rapid7.com/db

Анализ рисков информационной безопасности

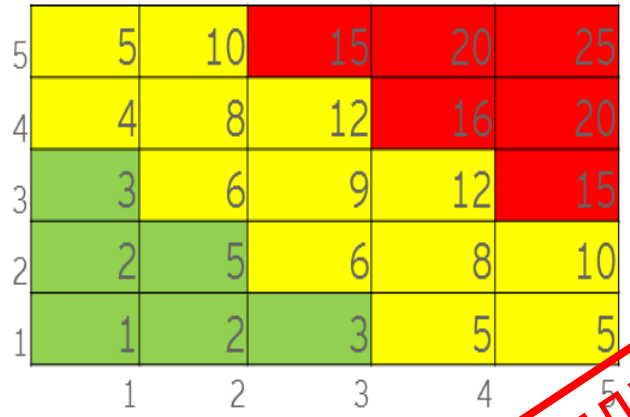
Основные понятия

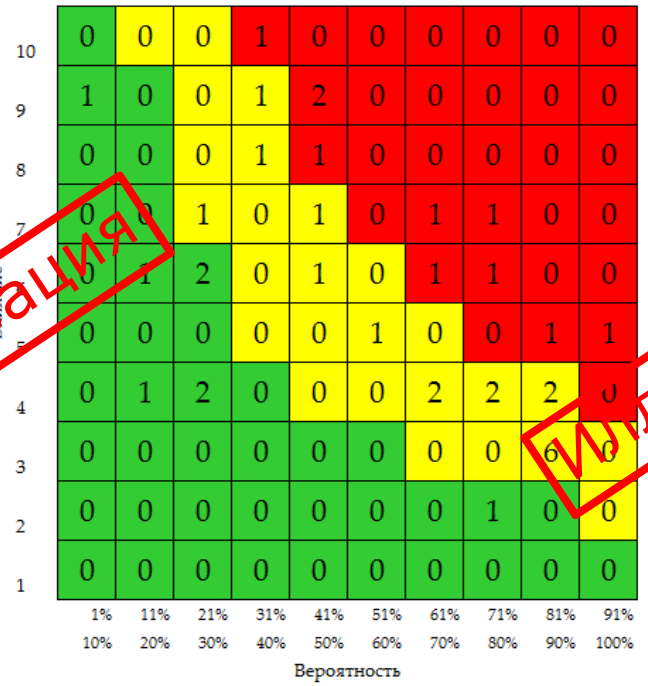
Риск информационной безопасности - это потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.

ВеличинаРиска = ВероятностьСобытия * РазмерУщерба, где

ВероятностьСобытия = ВероятностьУгрозы * ВеличинаУязвимости.

Примеры матрицы рисков информационной безопасности





Вероятность причинения вреда	Тяжесть последствий при причинении вреда				
	ОВТ	ВТ	СТ	НТ	НЗТ
Высокая вероятность (ВВ)	СВ	СВ	СВ	С	С
Средняя вероятность (СВ)	СВ	СВ	С	С	Н
Низкая вероятность (НВ)	СВ	С	С	Н	Н
Малая вероятность (МВ)	С	С	Н	Н	Н

Иллюстрация

Иллюстрация

Управление рисками информационной безопасности

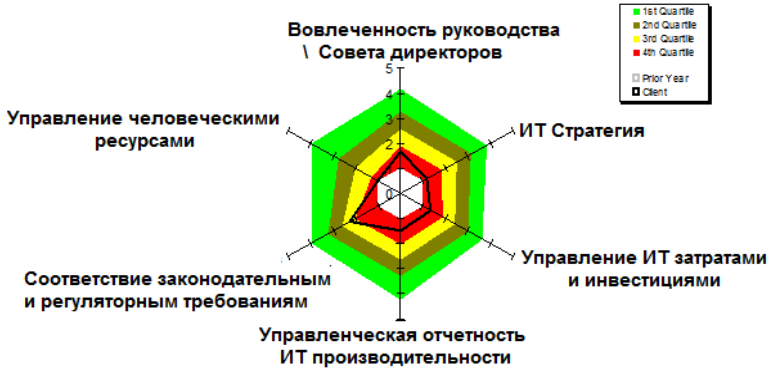
Управление рисками информационной безопасности

Кибер риски

Ключевые факторы оценки кибер рисков:

- Текущая роль ИБ фокусируется только на функции администрирования ПО и оборудования.
- Низкий уровень осведомленности сотрудников Банка в вопросах ИБ
- Даже при низком уровне автоматизации производства и бизнес процессов, ИТ инфраструктура и ее надежность остаются важными факторами успешности бизнеса.
- Приведенные значения показывают среднее значение по сравнению с финансовым сектором.

Контроли ИБ



Ключевые факторы зрелости ИБ процессов:

- Текущие возможности ИБ соответствуют низкому уровню зрелости и схож с низшими значениями по отрасли в целом.
- Самыми слабыми сторонами являются: Управление уязвимостями и мониторинга событий ИБ.
- Обеспечение непрерывности бизнеса немного лучше чем остальные области, однако не превышают средние значения по отрасли.

Иллюстрация

Карта соответствия кибер рисков и контролей

Области контроля	Контроли	Бизнес фокус	Информационные активы	Зависимость от ИТ	Зависимость от внутреннего ИТ персонала	Зависимость от третьих сторон	Надежность ИТ систем	Изменения в ИТ	Законодательные и регуляторные требования	Баллы по контролям
Управление ИТ	Вовлеченность руководства/совета директоров									2
	ИТ стратегия									1
	Управление ИТ затратами и инвестициями									2
	Управленческая отчетность ИТ производительности									2
	Соответствие законодательным и регуляторным требованиям									1
	Управление человеческими ресурсами									2
Управление проектами и изменениями	Методология разработки									1
	Управление проектами									1
	Участие пользователей									1
	Вычисления конечных пользователей									2
	Документация									1
	Бизнес управление изменениями									1
	Техническое управление изменениям									1
ИТ операции	Управление услугами третьих сторон									1
	Управление уровнем качества услуг									1
	Управление проблемами и инцидентами									3
	Операционное управление									1
	Управление конфигурациями									1
	Управление мощностями									1
Безопасность информации и систем	Политика безопасности									1
	Управление информационной безопасностью									1
	Контроль логического доступа									2
	Управление внешними коммуникациями									2
Непрерывность деятельности систем	Резервное копирование данных и систем									2
	Планирование непрерывности бизнеса									1
	Контроль физического доступа									3
	Защита физических объектов									3
Обеспечение контроля	Управление рисками									1
	ИТ аудит									1
	Контроль качества проекта									1
	Оценка адекватности контролей									1
Баллы по рискам		2	3	4	3	3	4	3	3	

Иллюстрация

Управление рисками информационной безопасности

SLE - single loss expectancy, ожидаемые разовые потери, т.е. «стоимость» одного инцидента.

ALE - annual loss expectancy, ожидаемые годовые потери, т.е. «стоимость» всех инцидентов за год.

EF - exposure factor, фактор открытости перед угрозой, т.е. какой процент актива будет поврежден угрозой при её успешной реализации.

ARO - annualized rate of occurrence, среднее количество инцидентов в год в соответствии со статистическими данными.

I – cost of investment, совокупные инвестиционные затраты на реализацию мер защиты

SLE=AssetValue*EF

ALE=SLE*ARO

(Ценность мер защиты для банка) = (ALE до внедрения мер защиты)

- (ALE после внедрения мер защиты) - (Ежегодные затраты на реализацию мер защиты).

ROIs = ALE – I / I

Q/A

Deloitte.