Security Management for Business

Раздел № 4

Информационная безопасность предприятия

Безопасность электронных ресурсов, систем и процессов

БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ РЕСУРСОВ, СИСТЕМ И ПРОЦЕССОВ

1. О соотношении понятий информационная и кибернетическая безопасность.
2. Философия информационной безопасности бизнеса.
3. Угрозы в сфере кибернетической безопасности бизнеса.
4. Системные угрозы кибернетической безопасности предприятия. Электронный шпионаж.
5. Деятельность отдельных лиц по нанесению ущерба кибернетической безопасности.
6. Уголовные преступления в сфере кибернетической безопасности.
7. Проблемы персонала и противодействие угрозам информационной безопасности бизнеса со стороны персонала.
8. Модели организации кибернетической безопасности предприятия.
9. Построение систем и аудит их эффективности.
10. Архитектура стандартов защиты информации и принципиальные подходы к их правовому обеспечению. Взаимодействие службы безопасности (через функцию информационной безопасности) с подразделением ИТ обеспечения предприятия.
11. Особенности подбора персонала, осуществляющего функцию обеспечения безопасности электронных ресурсов, систем и процессов.

СООТНОШЕНИЕ ПОНЯТИЙ ИНФОРМАЦИОННОЙ И КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

ОСНОВНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ ИНФОРМАЦИОННО-УДАРНЫХ ГРУППИРОВОК СИЛ И СРЕДСТВ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

- программное и информационное обеспечение
- программно-аппаратные, телекоммуникационные и другие средства информации и управления
- каналы связи, обеспечивающие циркуляцию информационных потоков и интеграцию системы управления
- интеллект человека и массовое сознание

ОСНОВНЫЕ ПРИЧИНЫ АКТУАЛИЗАЦИИ ПОНЯТИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

- ✓ **отсутствие международно-правовой основы запрещающей применение информационного оружия и проведение информационных операций;**
- ✓ **несовершенство нормативной правовой основы устанавливающей ответственность за совершение преступлений в сфере информационных технологий;**
- ✓ **разработка отдельными государствами доктрин и стратегий наступательных и подрывных действий в информационном пространстве;**
- ✓ **интенсивное развитие военных информационных технологий, в том числе средств поражения систем управления гражданского и военного назначения;**
- ✓ **нивелирование роли международных организаций и их органов, в области обеспечения международной информационной безопасности;**

ОСНОВНЫЕ ПРИЧИНЫ АКТУАЛИЗАЦИИ ПОНЯТИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

- ✓ создание и применение специальных сил и средств негативного воздействия на информационную инфраструктуру;
- ✓ существование специальных образцов вредоносного программного обеспечения поражающего автоматизированные системы управления промышленных и других объектов критически важной инфраструктуры;
- ✓ появление форм гражданского неповиновения связанных с посягательствами на информационную инфраструктуру в знак протеста против политики государства и деятельности органов власти;
- ✓ проникновение информационных технологий во все сферы государственной и общественной жизни, построение на их основе систем государственного и военного управления;
- ✓ развитие государственных проектов и программ в сфере информатизации (электронный документооборот, межведомственное электронное взаимодействие, универсальные электронные карты, предоставление государственных услуг в электронной форме) направленных на формирование информационного общества

УГРОЗЫ В СФЕРЕ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

Что такое кибернетические угрозы?

Кибернетические угрозы – явления, деяния, условия, факторы, представляющие опасность для информации управления, инфраструктуры управления, субъектов управления и порядка управления.

Опасность заключается в возможности нарушения свойств одного, либо нескольких указанных элементов, что может привести к нарушению управления.

УГРОЗЫ В СФЕРЕ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

О П А С Н О С Т Ь

- **ИНФОРМАЦИЯ ДЛЯ УПРАВЛЕНИЯ**
- **ИНФРАСТРУКТУРА УПРАВЛЕНИЯ**
- **СУБЪЕКТЫ УПРАВЛЕНИЯ**
- **ПОРЯДОК УПРАВЛЕНИЯ**

УГРОЗЫ В СФЕРЕ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

Изменение среды ведения бизнеса

Мобильность

Совместная работа

Виртуализация и облака

становятся причинами появления новых угроз

Угрозы сегодня

Устойчивые, сложные, мутирующие

Каждый экземпляр атаки может отличаться от другого

Домены меняются ежедневно, даже ежечасно

Контент мутирует и маскируется под легальный трафик

80% спама исходит от инцифицированных клиентов

70% «зомби» используют динамические IP-адреса

Угрозы из легальных доменов растут на сотни процентов в год

Спам составляет более 180 миллиардов сообщений в день

Эволюция угроз

Эволюция тактики реализации угроз

Смена ландшафта угроз

Зачем это надо злоумышленникам?!

Неужели это выгодно?!

- Партнерская сеть по продаже scareware
- Партнеры загружают scareware на зараженные компьютеры и получают комиссию 60% с продаж
- Объем продаж за десять дней $147K (154 825 установки и 2 772 продажи)
- $5M в год

Loader	Сетапы	Покупки	Покупки
37943	19989	667	29853.86
39895	19722	74	5420.64
41687	18619	384	28148.96
38059	16038	249	13908.24
39160	15335	176	9726.17
29968	12076	207	11672.71
13293	6866	129	6920.81
18055	8915	157	7557.25
29642	14802	265	12852.29
50457	22463	464	21055.29
338159	154825	2772	147116.22
Loads	Installs	Purchases	Total

Статистика продаж Bakasoftware за 10 дней

ТИПОВЫЕ СЦЕНАРИИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЭЛЕКТРОННЫМ СИСТЕМАМ И ПРЕВЕНТИВНАЯ ЗАЩИТА ОТ НИХ

ТИПОВЫЕ ПУТИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции;
- применение подслушивающих устройств (закладок);
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста принтера;
- хищение носителей информации и документальных отходов;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- мистификация (маскировка под запросы системы);
- использование программных ловушек;
- использование недостатков языков программирования и операционных систем;
- включение в библиотеки программ специальных блоков типа "Троянский конь";
- незаконное подключение к аппаратуре и линиям связи;
- злоумышленный вывод из строя механизмов защиты;
- внедрение и использование компьютерных вирусов.

ОСНОВНЫЕ ВИДЫ СЕТЕВЫХ АТАК

Почтовая бомбардировка
Атаки с подбором пароля
Вирусы, почтовые черви и "троянские кони"

Сетевая разведка
Производится сканирование портов, запросы DNS, эхо-тестирование раскрытых с помощью DNS адресов и т.д

Сниффинг пакетов
Сниффер перехватывает все сетевые пакеты, которые передаются через атакуемый домен.

IP-спуфинг - вид атаки, при которой хакер внутри организации или за ее пределами выдает себя за санкционированного пользователя.
IP-спуфинг часто используется как составная часть более сложной, комплексной атаки. Типичный пример — атака DDoS, для осуществления которой хакер обычно размещает соответствующую программу на чужом IP-адресе, чтобы скрыть свою истинную личность.

Атака на отказ в обслуживании
В случае атаки трафик, предназначенный для переполнения атакуемой сети, необходимо "отсекать" у провайдера услуг Интернет. Когда атака этого типа проводится одновременно через множество устройств, говорится о **распределенной атаке** DoS (Distributed Denial of Service — DDoS). Угрозу DoS-атак можно снизить несколькими способами. Во-первых, необходимо правильно сконфигурировать функции анти-спуфинга на маршрутизаторах и межсетевых экранах. Если хакер будет не в состоянии замаскировать свою истинную личность, он вряд ли решится на проведение атаки. Во-вторых, необходимо включить и правильно сконфигурировать функции анти-DoS на маршрутизаторах и межсетевых экранах. Также рекомендуется при угрозе DoS-атаки ограничить объем проходящего по Сети некритического трафика. Об этом уже нужно договариваться со своим Интернет-провайдером.

Атаки типа Man-in-the-Middle
Использование "дыр" и "багов" в ПО

Электронные финансы, системы банк-клиент и электронный банк, их защита от противоправных посягательств.

Самый популярный вектор атаки – на компьютер клиента банка с последующим хищением или использованием ключа его электронно-цифровой подписи (ЭЦП) и перехватом логина и пароля учетной записи в системе «интернет-банк». Ситуацию усугубляет использование однотипного программного обеспечения для доступа к ДБО.

Фактически банк не может влиять на безопасность клиента! Максимум, что обычно может сделать банк – это навязать клиенту USB-Token и выполнить привязку его IP-адреса. Кроме того, придумываются различные алгоритмы двухфакторной авторизации, вроде использования карточки одноразовых паролей или SMS - уведомлений.

Если рабочая станция с «банк-клиентом» будет отделена межсетевым экраном от локальной сети, если доступ с этой рабочей станции возможен только на IP-адрес банка, если удалить с этого компьютера все ненужное ПО и не держать USB-Token постоянно включенным в компьютер, то это снизит риски практически до минимума

ДВЕ ТИПОВЫЕ МОДЕЛИ ПОВЕДЕНИЯ НАРУШИТЕЛЯ

1. «Классический хакер» сканирует сервисы, ищет устаревшую версию используемого ПО, слабости и уязвимости в системе аутентификации, и, конечно же, уязвимости в доступных web-приложениях – самом слабом, по статистике, звене системы дистанционного банковского обслуживания. Но от такого нарушителя достаточно легко защититься, да и обнаружить его деятельность также не является проблемой.
2. Гораздо опаснее вторая модель, когда нарушитель является законным пользователем системы, когда у него есть своя учетная запись, свой счёт и все права на него. Вот только в отличие от обычного пользователя он пытается исследовать систему в надежде найти уязвимости.

CROSS-SITE SCRIPTING

Такая уязвимость позволяет атакующему влиять на генерируемое содержимое web-страницы системы интернет-банк. Таким образом, злоумышленник может использовать ресурс банка для атаки на клиента, например, изменив страницу так, как если бы она выглядела при аутентификации в системе. Такая атака называется «Фишинг» . В сочетании с уязвимостью XSS эта атака становится более опасной, так как домен и IP-адрес действительно принадлежат банку.

SQL-ИНЪЕКЦИЯ

Она позволяет злоумышленнику общаться с базой данных системы интернет-клиент в обход правил системы, что, в итоге, может привести к утечке (или в некоторых случаях – к изменению) базы клиентов, их счетов, номеров пластиковых карт, платежных поручений, паролей от системы, и т.п.

ОШИБКИ БИЗНЕС ЛОГИКИ

Пример: при конвертации валюты скрипт генерирует курс и просит пользователя ввести сумму, которую он хочет обменять. Если при этом не происходит дополнительной проверки курса, то злоумышленник может поменять курс по своему усмотрению, из-за чего конвертация может пройти с неправильным курсом.

Электронные финансы, системы банк-клиент и электронный банк, их защита от противоправных посягательств.

ОСНОВНАЯ СХЕМА МОШЕННИЧЕСКИХ МАХИНАЦИИЙ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ БАНК-КЛИЕНТОВ

1. Хаотичное заражение большого количества ПК вредоносным программным обеспечением, использую незакрытые уязвимости в браузерах или др. прикладном ПО (часто используются незакрытые дыры в ПО Adobe, Microsoft, Mozilla и д.р.).
2. Если в список зараженных ПК попадает машина, с которой осуществляются банковские операции, данный факт регистрируется, и на нее закачиваются дополнительные модули, необходимые для кражи электронных ключей и аутентификационной информации. Часто применяются различные кейлоггеры, средства удаленного управления (Teamviewer, VNC, Remote Admin), вредоносные модули, предназначенные специально для извлечения ключей из реестра и внешних носителей.
3. Как только необходимая информация собирается, она передается злоумышленникам, которые проверяют возможность авторизации и проведения платежных поручений.
4. Как только вся необходимая информация для проведения мошенничества готова, злоумышленники прилагают усилия для того, чтобы скрыть следы преступления от жертвы. Применяются различные методы, начиная от нарушения функционирования ПК, с которого были похищены ключи, заканчивая DDoS-атаками на сервер банк-клиента. Цель данных действий – максимально отсрочить момент обнаружения факта преступления, чтобы деньги успели перевестись на подставные фирмы.
5. Деньги выводятся через цепочку счетов подставных компаний или пластиковые карточки физических лиц. Наиболее часто обналичивание производится в районе Урала и Западной Сибири, регулярно мелькают такие города, как Екатеринбург, Челябинск и др.

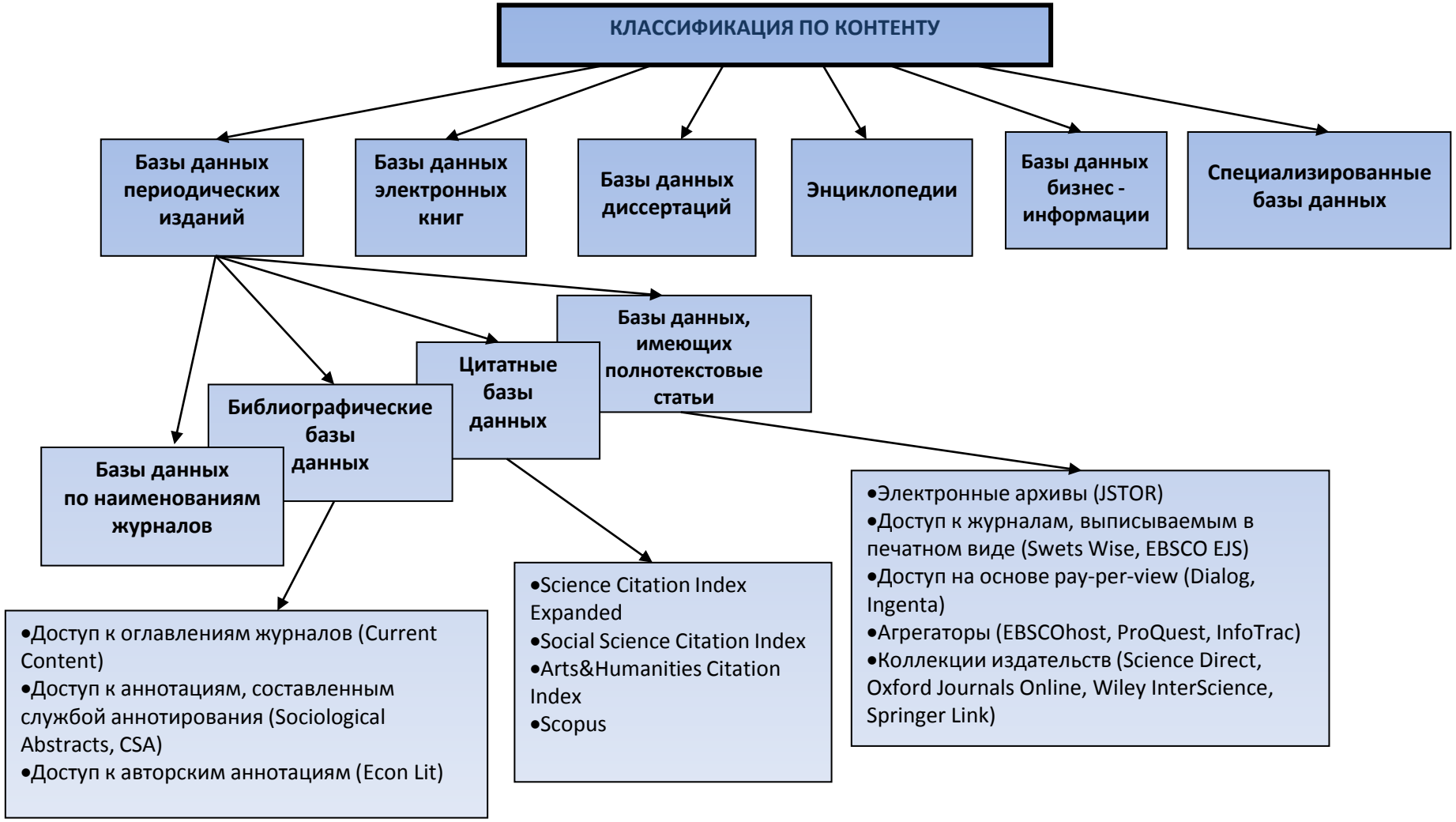
ОСНОВНЫЕ ПРИЧИНЫ УСПЕХА МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

1. **Недостаточное внимание клиентов банка к информационной безопасности. Недостаточная компьютерная грамотность персонала, работающего с ДБО. Игнорирование рекомендаций и лучших практик по защите информации и организации бизнес-процессов.**

2. **Применение дискет и флеш-накопителей, а также ключей реестра для хранения ключевой информации вместо токенов. Отсутствие процедуры аутентификации по одноразовым паролям. Отсутствие разграничения доступа к счетам по IP-адресу клиента.**

3. **Неэффективная работа anti-fraud систем и процедур в банках. Отсутствие или некорректная работа процедуры валидации получателя платежа, отсутствие мониторинга профиля финансовой активности клиента с целью выявления подозрительных транзакций, отсутствие межбанковского обмена информацией по мошенничествам.**

ИНФОРМАЦИОННЫЕ РЕСУРСЫ – ОТДЕЛЬНЫЕ ДОКУМЕНТЫ И МАССИВЫ ДОКУМЕНТОВ В БИБЛИОТЕКАХ, АРХИВАХ, ФОНДАХ, БАНКАХ ДАННЫХ И ДРУГИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ.



МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

КРИПТОГРАФИЯ

Количество возможных ключей для алгоритма зависит от числа бит в ключе. Например,8-битный ключ допускает 256 (2^8) комбинаций ключей. Чем больше возможных комбинаций ключей, тем труднее подобрать ключ, тем надёжнее зашифровано послание. Так, например, если использовать 128-битный ключ, то необходимо будет перебрать 2^{128} ключей, что в настоящее время не под силу даже самым мощным компьютерам.

СИММЕТРИЧНОЕ ШИФРОВАНИЕ

отправитель и получатель владеют одним и тем же ключом (секретным), с помощью которого они могут зашифровывать и расшифровывать данные.

Недостатки:

- очень сложно найти безопасный механизм, при помощи которого отправитель и получатель смогут тайно от других выбрать ключ. Возникает проблема безопасного распространения секретных ключей;
- для каждого адресата необходимо хранить отдельный секретный ключ;
- в схеме симметричного шифрования невозможно гарантировать личность отправителя, поскольку два пользователя владеют одним ключом.

ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ

для шифрования послания используются два различных ключа. При помощи одного из них послание зашифровывается, а при помощи второго – расшифровывается.

Недостатки:

необходимость использования более длинных, чем при симметричном шифровании, ключей для обеспечения эквивалентного уровня безопасности, что сказывается на вычислительных ресурсах, требуемых для организации процесса шифрования.

ЭЛЕКТРОННАЯ ПОДПИСЬ

*Электронные подписи создаются **шифрованием контрольной суммы и дополнительной информации при** помощи личного ключа отправителя. Таким образом, кто угодно может расшифровать подпись, используя открытый ключ, но корректно создать подпись может только владелец личного ключа. Для защиты от перехвата и повторного использования подпись включает в себя уникальное число – порядковый номер. При помощи электронной подписи получатель может убедиться в том, что полученное им сообщение послано не сторонним лицом, а имеющим определённые права отправителем.*

АУТЕНТИФИКАЦИЯ

Схема ЛОГИН – ПАРОЛЬ

Схема ОДНОРАЗОВЫЕ ПАРОЛИ

Схема S/Key

Биометрическая аутентификация

ПЕРСПЕКТИВЫ В ДЕЛЕ ЗАЩИТЫ ОТ НСД

1. Акцент при построении защитных систем будет плавно перемещаться — от противодействия "внешним" хакерским нападениям к защите от нападений "изнутри".

2. Будут развиваться и совершенствоваться аппаратные средства защиты от хакерских атак. На рынке появится новый класс сетевого оборудования — "защитные сервисные коммутаторы". Они смогут обеспечивать комплексную защиту компьютерных сетей, тогда как современные устройства обычно выполняют довольно ограниченный набор конкретных функций, а основная тяжесть все равно ложится на специализированное программное обеспечение.

3. Стремительное развитие обеспечено рынку услуг по защищенной доставке цифрового контента и защите самого контента от нелегального копирования и несанкционированного использования.

4. Гораздо шире будут применяться системы биометрической аутентификации (по сетчатке глаза, отпечаткам пальцев, голосу и т.д.), в том числе и комплексные.

5. Львиную долю услуг безопасности будут оказывать своим клиентам Интернет-провайдеры. Причем основными их клиентами станут компании, бизнес которых строится именно на интернет-технологиях, то есть активные потребители услуг web-хостинга, систем электронной коммерции и т.д.

6. Быстрый рост ожидает рынок интеллектуальных услуг сетевой защиты. Это связано с тем, что новые концепции защиты IT-систем от хакеров акцентируют внимание не столько на реагирование на уже произошедшие события/атаки, а на их прогнозирование, предупреждение и проведение упреждающих и профилактических мероприятий.

7. Существенно повысится спрос на коммерческие системы криптошифрования передаваемых данных, включая "индивидуальные" разработки для конкретных компаний с учетом их сфер деятельности.

8. На рынке решений по IT-безопасности будет происходить постепенный отход от "систем стандартной комплектации", в связи с чем возрастет спрос на консалтинговые услуги по разработке концепций информационной безопасности и построению систем управления информационной безопасностью для конкретных заказчиков.

Индустрия киберпреступности похожа на ИТ

- Высокообразованные специалисты взаимодействуют между собой для создания новых вредоносных программ
- Для управления большими проектами используются специализированные средства разработки ПО, контроля версий и взаимодействия разработчиков
- Разработчики вредоносных программ ничем не отличаются от таких же в ИТ-индустрии
- Обмен информацией и талантами при совместной работе дает гораздо больший эффект, чем работа в одиночку
- Большие заработки не оставляют надежды на самостоятельное прекращение этого бизнеса

Что делать?

- Это уже не детские шалости и бороться в одиночку с этой проблемой потребители не в состоянии
- Технические средства также не в состоянии решить эту проблему
  - В цикле «проактивные действия – активная защита – реагирование» технические решения направлены, как правило, на вторую стадию
- Любой бизнес может быть прекращен или снижен его масштаб устранив основные причины его возникновения и способы получения прибылей
  - Если удастся заблокировать перевод украденных денежных средств, то у киберпреступников пропадут стимулы участвовать в данной бизнес-модели
- Нужно сделать киберпреступление дорогим или опасным
  - Это выбьет почву из под ног киберпреступников

ДЕЯТЕЛЬНОСТЬ ЛИЦ ПО НАНЕСЕНИЮ УЩЕРБА КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

Популярный пример жизненного цикла киберпреступности

1. Разработка и тестирование вредоносного кода
2. Вредоносный код объявляется к продаже
3. Вредоносный код размещается на различных сайтах
   - Сайты могут быть как специально подготовленные, так и общепопулярные, но взломанные
4. Вредоносный код загружается на компьютеры пользователей при посещении зараженных сайтов
   - В случае специально подготовленных сайтов используются партнерские схемы pay-per-install
5. Вредоносный код собирает информацию для продажи (учетные записи, персональные данные, ключи электронной подписи и т.д.)
6. Собранная информация используется или продается

Ключевые виды деятельности

- Производство
- Разрешение проблем
- Платформы/сети

Ключевые партнеры

- Оптимизация и экономия в сфере производства
- Снижение риска и неопределенности
- Поставки ресурсов и совместная деятельность

- Типы партнеров
  - Abuse-хостеры
  - Гаранты
  - Владельцы ботнетов
  - Владельцы анонимных прокси
  - Владельцы Fast-Flux-хостинга
  - Продавцы трафика
  - И т.д.

ПЕРСОНАЛ

У каждого своя роль

- Менеджер по продажам
- Кассир
- Маркетолог
- Логист
- Водитель
- HR
- Генеральный директор
- Айтишник
- Охранник
- Инженер
- Разработчик
- Дроп (разводной / неразводной)
- Дроповод
- Обнальщик
- Заливщик / Даунлоадер
- Селлер
- Abuse-хостер
- Гарант
- Кодер

МОТИВЫ КИБЕРПРЕСТУПЛЕНИЙ

Деньги играют важную роль, но есть и другие мотивы

	Кибер-террористы	Кибер-воины	Хактивисты	Писатели malware	Старая школа	Фрикеры	Самураи	Script kiddies	Warez D00dz
Сложность				+	+	+	+		+
Эго				+	+	+			+
Шпионаж		+		+					
Идеология	+	+	+		+				+
Шалость				+		+		+	
Деньги		+		+		+	+		+
Месть	+		+	+				+	

Источник: Furnell, S. M

- Отсутствие желания заработать не означает отсутствие бизнес-модели киберпреступности
  - Anonymous, Lulzsec демонстрируют это в полной мере

УГОЛОВНЫЕ ПРЕСТУПЛЕНИЯ В СФЕРЕ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

УГОЛОВНЫЕ ПРЕСТУПЛЕНИЯ В СФЕРЕ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

ОБЩЕУГОЛОВНЫЕ ПРЕСТУПЛЕНИЯ В СФЕРЕ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

Ст. 158	**Кража – тайное хищение чужого имущества**
Ст. 159	**Мошенничество – хищение чужого имущества путем обмана, или злоупотребления доверием**
Ст. 159.3	**Мошенничество с использованием платежных карт**
Ст. 159.4	**Мошенничество в сфере предпринимательской деятельности**
Ст. 159.6	**Мошенничество в сфере компьютерной информации – хищение чужого имущества путем ввода, удаления, блокирования, модификации компьютерной информации, либо иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации**
Ст. 165	**Причинение имущественного ущерба путем обмана или злоупотребления доверием**
Ст. 167	**Умышленное уничтожение или повреждение имущества**
Ст. 171	**Незаконное предпринимательство**
Ст. 171.2	**Незаконная организация и проведение азартных игр**
Ст. 172	**Незаконная банковская деятельность**
Ст. 183	**Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую, или банковскую тайну**

ОСНОВНЫЕ ИСТОЧНИКИ ПРОБЛЕМ ПЕРСОНАЛА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОММУНИКАТИВНЫЕ ОСОБЕННОСТИ

Люди склонны обсуждать свои животрепещущие проблемы с коллегами везде, где только можно, – от столовой до вагона метро. В последние годы бороться с этой человеческой слабость стало сложнее, поскольку ушли в прошлое традиции секретности.

КОГНИТИВНЫЕ СПОСОБНОСТИ

Человек, в отличии машин, способен воспринимать и обобщать информацию, поступающую из различных альтернативных источников, таких, как чужие телефонные разговоры, проекты документов на столе коллег, слухи и сплетни, обрывки фраз или просто настроение руководства.

ЛИЧНОСТНЫЕ КАЧЕСТВА

Люди обижаются, и порой мстят, и нанесение вреда информационным ресурсам стало одним из популярных способов отмщения обидчикам. Следует помнить, что можно не только запускать вирусы в корпоративные сети или стирать файлы – порой не меньший вред можно причинить, положив не на то место дело или бумажный документ, или же просто не поделившись известной человеку информацией.

ОСОБЕННОСТИ ТИПА «ХОЧУ ВСЕ ЗНАТЬ»

Ограничения доступа к информации (особенно непродуманные) воспринимаются как вызов, и побуждают людей к активным, порой весьма хитроумным действиям по их преодолению или обходу.

ДЕФИЦИТ КВАЛИФИЦИРОВАННЫХ СПЕЦИАЛИСТОВ

В отличие от машин, квалифицированные сотрудники не выпускаются на конвейере, и найти полноценную замену заболевшему или уволившемуся работнику не всего просто. Ситуация может стать очень острой, если выбывшего сотрудника некому подстраховать.

ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СО СТОРОНЫ ПЕРСОНАЛА

У информационной безопасности большинства предприятий оказывается «семь нянек»: ***администрация, служба обработки документов (ДОУ), служба безопасности, служба персонала, ИТ служба, юридический отдел, деловые подразделения.***

Виды операций	Информационные ресурсы		
	Бумажные документы	Электронные документы	Информация и знания сотрудников
Создание информационного ресурса (создание и оформление документов)	Деловые подразделения	Деловые подразделения	Деловые подразделения
Ввод документов в систему делопроизводства	ДОУ и деловые подразделения	Деловые подразделения	
Оперативная работа с документами и документационное обеспечение деловых процессов	Деловые подразделения, ДОУ	Деловые подразделения, ИТ	?
Организация документооборота	ДОУ	ИТ?	-
Обеспечение соответствия требованиям законодательства	СВК, ДОУ, юридический отдел	?	Руководство, СП и СБ ?
Учет документов (ознакомленности с информацией)	ДОУ	?	?
Контроль исполнения	ДОУ	ДОУ?	-
Определение сроков хранения документов	ДОУ, юридический отдел, деловые подразделения	?	-
Проведение экспертизы ценности документов и информации	ДОУ, юридический отдел, деловые подразделения	?	?
Уничтожение документов с оформлением акта	ДОУ и СБ	?	-
Резервирование документов и информации	ДОУ	ИТ	?
Долговременное хранение документов с сохранением их целостности и аутентичности; передача профессионального опыта и знаний	ДОУ	ИТ ?	?
Управление доступом	ДОУ	ИТ	?
Физическая защита (обеспечение наличия ресурса)	ДОУ и СБ	ИТ и СБ	Руководство, СП и СБ
Защита важнейших документов	ДОУ?	ИТ?	?
Защита конфиденциальной информации и персональных данных	ДОУ, СБ, юридический отдел и деловые подразделения	СБ, ИТ и деловые подразделения	Руководство, СП и СБ
Сохранение корпоративной памяти	ДОУ	?	?
Обучение правилам и методам работы (использования ресурса)	ДОУ	ИТ	СП, СБ, ДОУ

ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СО СТОРОНЫ ПЕРСОАЛА

ТИПОВЫЕ РАЗНОВИДНОСТИ УТЕЧЕК, СВЯЗАННЫХ С ПЕРСОНАЛОМ КОМПАНИИ

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ СЛУЖБЫ ПЕРСОНАЛА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕСА:

1. ПОДБОР НАДЁЖНЫХ И ВЫСОКОКВАЛИФИЦИРОВАННЫХ РАБОТНИКОВ;
2. ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ;
3. ЗАЩИТА ИНФОРМАЦИИ, НАХОДЯЩЕЙСЯ В ГОЛОВАХ СОТРУДНИКОВ И ИМЕЮЩЕЙ ЦЕННОСТЬ ДЛЯ ОРГАНИЗАЦИИ, В КОТОРОЙ ОНИ РАБОТАЮТ.

ДАННЫЕ ЕЖЕГОДНОГО ОПРОСА КОММЕРЧЕСКИХ ФИРМ, ПРОВОДИМОГО СОВМЕСТНО ИНСТИТУТОМ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ (COMPUTER SECURITY INSTITUTE – CSI) И ФБР

56% - заметили несанкционированный доступ к своим компьютерам,
30% - сообщили о попытках взлома «изнутри».

В качестве основных причин для беспокойства компании отметили:

97% - злоупотребление сетевым доступом со стороны сотрудников,
94% - заражение вирусами,
71% - несанкционированный доступ «изнутри»
69% - кража ноутбуков.

ДАННЫЕ ИССЛЕДОВАНИЙ ИБ В 2011 Г. КОМПАНИИ «CISCO»

70% молодых сотрудников, знакомых с корпоративными ИТ - правилами, признали, что нарушают эти правила с большей или меньшей регулярностью. При этом: каждый третий нарушитель не видит в этом ничего страшного,
22% опрошенных заявили, что доступ к несанкционированным программам и приложениям им нужен для выполнения своих профессиональных обязанностей,
19% признали, что корпоративные ИТ - правила в их компаниях не соблюдаются,
18% сказали, что во время работы им не до того, чтобы об этих правилах думать,
16% считают такие правила неудобными,
15% о корпоративных ИТ - правилах попросту забывают,
14% оправдывают свое поведение тем, что, мол, начальники за ними все равно не следят,

ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СО СТОРОНЫ ПЕРСОНАЛА

ИЗ СТАНДАРТА БАНКА РОССИИ «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ»

5.2. Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал.

5.8. Соблюдение политики ИБ в значительной степени является элементом корпоративной этики, поэтому на уровень ИБ в финансовой организации оказывают серьезное влияние отношения, как в коллективе, так и между коллективом и собственником или менеджментом организации, представляющим интересы собственника. Поэтому этими отношениями необходимо управлять. Необходимо обучение и регулярная переподготовка кадров, как по основной деятельности, так и по вопросам информационных технологий, делопроизводства и безопасности.

10.7. Обязательны краткие занятия с работниками организации по вопросам обеспечения ИБ и введение аттестации персонала по вопросам обеспечения безопасности.

ИЗ СТАНДАРТА ISO 17779 «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ»:

- Условия найма должны определять обязанности и ответственность сотрудника за информационную безопасность. При необходимости, такая ответственность должна сохраняться в течение определенного времени после увольнения сотрудника. Должны быть также указаны действия, предпринимаемые в том случае, если сотрудник пренебрегает требованиями к информационной безопасности.

- В тех случаях, когда должностные обязанности, как при первоначальном поступлении на работу, так и в результате продвижения по службе, предусматривают доступ к средствам обработки информации, особенно к средствам обработки конфиденциальной информации, например, финансовой или секретной, – организация должна также проверить финансовое положение сотрудника. Занимающие ответственные посты сотрудники должны проходить такую проверку регулярно.

- Обучение и подготовка по вопросам информационной безопасности (п. 6.2.1.). Все сотрудники организации, а при необходимости, и пользователи из сторонних организаций, должны пройти обучение по используемым в организации регламентам и процедурам, и регулярно получать информацию об изменениях в них. Такая программа подготовки затрагивает требования к обеспечению безопасности, вопросы юридической ответственности и средства управления деловыми процессами, а также включает обучение правильному использованию средств обработки информации (например, процедуре входа в систему, использованию программного обеспечения), – прежде чем будет предоставлен доступ к информации и средствам её обработки.

МОДЕЛИ ОРГАНИЗАЦИИ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

ПОЛИТИКА БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ - совокупность руководящих принципов, правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности (ГОСТ Р ИСО/МЭК 15408)

МОДЕЛЬ БЕЗОПАСНОСТИ - формальное (*математическое*, *алгоритмическое*, *схемотехническое* и т.п.) выражение политики безопасности

Модель безопасности служит для:

- ✓выбора и обоснования базовых принципов архитектуры, определяющих механизмы реализации средств защиты информации
- ✓подтверждения свойств (защищенности) разрабатываемой системы путем формального доказательства соблюдения политики (требований, условий, критериев) безопасности
- ✓оставления формальной спецификации политики безопасности разрабатываемой системы

Основные требования к моделям обеспечения кибернетической безопасности

CIA (Confidentiality, Integrity, and Availability — конфиденциальность, целостность и доступность).
Эти три группы принципов являются общепризнанными при оценке рисков, связанных с важной информацией, и при утверждении политики безопасности.

Конфиденциальность — Важная информация должна быть доступна только ограниченному кругу лиц.
Целостность — Изменения информации, приводящие к её потере или искажению, должны быть запрещены.
Доступность — Информация должна быть доступна авторизованным пользователем, когда она им необходима.

МОДЕЛИ ОРГАНИЗАЦИИ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

МОДЕЛЬ ИЗБИРАТЕЛЬНОГО (ДИСКРЕЦИОННОГО) ДОСТУПА

Множество потоков информации, характеризующих легальный доступ, задается явным образом внешним по отношению к системе фактором в виде указания дискретного набора троек "субъект-поток(операция)-объект":

✓права доступа предоставляются (*«прописываются» в специальных информационных объектах-стуктурах*), отдельно каждому пользователю к тем объектам, которые ему необходимы для работы в КС;
✓при запросе субъекта на доступ к объекту диспетчер, обращаясь к ассоциированным с ним информационным объектам, в которых «прописана» политика разграничения доступа, определяет «легальность» запрашиваемого доступа и разрешает/отвергает доступ.

Достоинства дискреционных моделей:

•*Хорошая детализация защиты* (*позволяют управлять доступом с точностью до отдельной операции над отдельным объектом*)
•*Простота реализации*

Недостатки дискреционных моделей:

•*Слабые защитные характеристики из-за невозможности для реальных систем выполнять все ограничения безопасности*
•*Проблема "троянских коней"*
•*Сложности в управлении доступом из-за большого количества назначений прав доступа*

МОДЕЛИ ОРГАНИЗАЦИИ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

МОДЕЛЬ ПОЛНОМОЧНОГО (МАНДАТНОГО) ДОСТУПА

Множество потоков информации, характеризующих легальный доступ, задается неявным образом через предоставление субъектам неких полномочий (допуска, мандата) порождать определенные потоки над объектами с определенными характеристиками конфиденциальности (метками, грифами секретности):

Основаны:

✓на *субъектно-объектной* модели КС

✓на *правилах организации секретного делопроизводства*, принятых в государственных учреждениях многих стран.

Информация (точнее документы, ее содержащие) категорируется специальными метками конфиденциальности – т.н. ***грифы секретности*** документов

Сотрудники по уровню благонадежности (доверия к ним) получают т.н. ***допуски*** определенной ***степени***

Сотрудники с допуском определенной степени приобретают ***полномочия*** работы с документами определенного грифа секретности

Главная задача: не допустить утечки информации из документов с высоким грифом секретности к сотрудникам с низким уровнем допуска

Достоинства моделей мандатного доступа

•*ясность и простота реализации*

•*отсутствие проблемы "Троянских коней" (контролируется направленность потоков, а не взаимоотношения конкретного субъекта с конкретным объектом, поэтому недекларированный поток троянской программы «сверху-вниз» будет считаться опасным и отвергнут МБО)*

•*каналы утечки не заложены в саму модель, а могут возникнуть только в практической реализации*

Недостатки моделей мандатного доступа

•*возможность скрытых каналов утечки - механизм, посредством которого субъект с высоким уровнем безопасности м. предоставить определенные аспекты конфиденциальной информации субъекту, уровень безопасности которого ниже уровня безопасности конфиденциальной информации*

•*проблема удаленного доступа. В распределенных системах осуществление доступа всегда сопровождается потоком информации в прямом и обратном направлении, что в результате может приводить к нарушениям привил NRU и NWD*

•*проблема избыточности прав доступа. Без учета матрицы доступа (т.е. без использования дискреционного доступа) мандатный принцип доступа организует доступ более жестко, но и более грубо, без учета потребностей конкретных пользователей-субъектов*

МОДЕЛИ ОРГАНИЗАЦИИ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

МОДЕЛЬ РОЛЕВОГО (ТИПИЗОВАННОГО) ДОСТУПА

Множество потоков информации, характеризующих легальный доступ, задается через введение в системе дополнительных абстрактных сущностей – ролей, с которыми ассоциируются конкретные пользователи, и наделение ролевых субъектов доступа на основе дискреционного или мандатного принципа правами доступа к объектам системы.

Основная идея: политика и система защиты должны учитывать ***организационно-технологическое взаимодействие пользователей.*** *(Впервые была применена в продуктах управления доступом корпорации IBM в 70-80.гг.)*

Вместо субъекта

- ***пользователь*** (конкретная активная сущность)
- ***роль*** (абстрактная активная сущность)

Неформально ***Роль***: типовая работа в КС (ИС) определенной группы пользователей

Аналог: нормативное положение, функциональные обязанности и права сотрудников по определенной должности, *например могут быть роли* - кассира, бухгалтера, делопроизводителя, менеджера и т.п.

Наиболее распространены модели с иерархической системой ролей:

- чем выше роль по иерархии, тем больше полномочий
- если пользователю присвоена какая-то роль, то ему автоматически присваиваются все роли ниже по иерархии

MMS (military message system)-модель

Основная схема функционирования системы - пользователи после ***идентификации*** запрашивают у системы операции над сущностями от своего ***ID*** или от имени ***Роли***, с которой в данный момент ***авторизован.***

Модель Лендвера-Маклина (MMS) сочетает принципы: ***ролевой, дискреционной и мандатной моделей*** и оказывает сильное влияние на модели и технологии современных защищенных КС.

ПОСТРОЕНИЕ СИСТЕМ И АУДИТ ИХ ЭФФЕКТИВНОСТИ

ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Профилактика возможных угроз. Необходимо своевременное выявление возможных угроз безопасности предприятия, анализ которых позволит разработать соответствующие профилактические меры.

***Законность*.** Меры по обеспечению безопасности разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

***Комплексное использование сил и средств*.** Для обеспечения безопасности используются все имеющиеся в распоряжении предприятия силы и средства. Каждый сотрудник должен, в рамках своей компетенции, участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является программа (план работ) обеспечения безопасности предприятия.

Координация и взаимодействие внутри и вне предприятия. Меры противодействия угрозам осуществляются на основе взаимодействия и координации усилий всех подразделений, служб предприятия, а также установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия.

***Сочетание гласности с секретностью*.** Доведение информации до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль - предотвращение потенциальных и реальных угроз.

Компетентность. Сотрудники должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям.

Экономическая целесообразность. Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

Плановая основа деятельности. Деятельность по обеспечению безопасности должна строиться на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам (экономическая, научно - техническая, экологическая, технологическая и т. д.) и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников.

ПОСТРОЕНИЕ СИСТЕМ И АУДИТ ИХ ЭФФЕКТИВНОСТИ

Различают два основных вида аудита: ***внутренний*** (проводимый исключительно силами сотрудников предприятия) и ***внешний*** (осуществляемый сторонними организациями).

ОСНОВНЫМИ ЦЕЛЯМИ АУДИТА ЯВЛЯЮТСЯ:

✓установление степени защищенности информационных ресурсов предприятия, выявление недостатков и определение направлений дальнейшего развития системы защиты информации;
✓проверка руководством предприятия и другими заинтересованными лицами достижения поставленных целей в сфере информационной безопасности, выполнения требований политики безопасности;
✓контроль эффективности вложений в приобретение средств защиты информации и реализацию мероприятий по обеспечению информационной безопасности;
✓сертификация на соответствие общепризнанным нормам и требованиям в сфере информационной безопасности (в частности на соответствие национальным и международным стандартам).

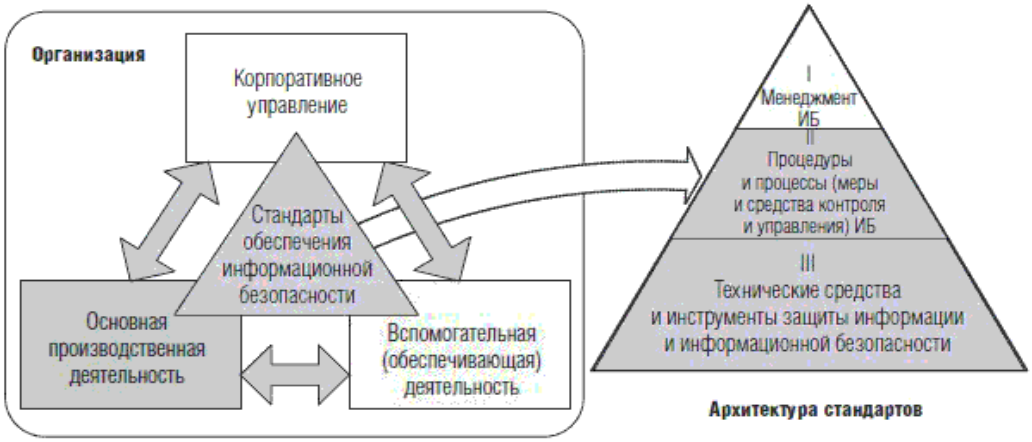
ОСНОВНЫЕ ЭТАПЫ ПРОВЕДЕНИЯ АУДИТА:
✓инициирование проведения аудита;
✓непосредственно осуществление сбора информации и проведение обследования аудиторами;
✓анализ собранных данных и выработка рекомендаций;
✓подготовка аудиторского отчета и аттестационного заключения.

В случае, если аудит не является ***комплексным***, на начальном этапе необходимо определить его непосредственные границы:
✓перечень обследуемых информационных ресурсов и информационных систем;
✓перечень зданий, помещений и территорий, в пределах которых будет проводиться аудит;
✓основные угрозы, средства защиты от которых нужно подвергнуть аудиту;
✓элементы системы обеспечения информационной безопасности, которые необходимо включить в процесс проверки.

Основная стадия – ***проведение аудиторского обследования и сбор информации*** - как правило, должно включать в себя:
✓анализ имеющейся политики информационной безопасности и другой организационной документации;
✓проведение совещаний, опросов, доверительных бесед и интервью с сотрудниками предприятия;
✓проверку состояния физической безопасности информационной инфраструктуры предприятия;
✓техническое обследование информационных систем – программных и аппаратных средств (инструментальная проверка защищенности).

АРХИТЕКТУРА СТАНДАРТОВ ЗАЩИТЫ ИНФОРМАЦИИ

ОБОБЩЕННАЯ АРХИТЕКТУРА СТАНДАРТОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ



К категории I («Менеджмент ИБ») относятся стандарты семейства менеджмента ИБ ISO/IEC 270XX (семейство стандартов СМИБ организации), и комплекс новых стандартов направления Identity management and privacy technologies (менеджмент идентификационными атрибутами и безопасность личности в электронном мире). Среди российских национальных стандартов к данной категории можно отнести только гармонизированные международные.

К категории II («Процедуры и процессы ИБ») можно отнести стандарты для следующих объектов и аспектов стандартизации:
- менеджмент инцидентов информационной безопасности;
- безопасность сетей информационных технологий;
- обнаружение вторжений, выбор и поставка систем обнаружения вторжений;
- управление и пользование услугами третьей доверенной стороны;
- восстановление информационных технологий после бедствий и аварий и т. п.
- Среди российских национальных стандартов к данной категории можно отнести ГОСТ Р 50922, ГОСТ Р 51275 и др.

К категории III («Технические средства и инструменты защиты информации и информационной безопасности») можно отнести стандарты на алгоритмы криптографических преобразований, критерии оценки безопасности информационных технологий и т. п.
Среди российских национальных стандартов к данной категории можно отнести стандарты требований по защите от несанкционированного доступа к средствам вычислительной техники и автоматизированным системам, гармонизированные международные стандарты критериев оценки безопасности информационных технологий (ГОСТ Р ИСО/МЭК 15408), ГОСТ Р ИСО/МЭК 18045), защиты от вредоносного программного обеспечения и т. п.

ВЗАИМОДЕЙСТВИЕ СЛУЖБЫ БЕЗОПАСНОСТИ С ПОДРАЗДЕЛЕНИЯМИ ИТ ОБЕСПЕЧЕНИЯ ПРЕДПРИЯТИЯ.

ОСНОВА ВЗАИМОДЕЙСТВИЯ – ПРАВИЛО ДВУХ КЛЮЧЕЙ

СПЕЦИАЛЬНЫЕ ФУНКЦИИ ОБЕСПЕЧЕНИЯ ИБ

•***определять*** критерии, по которым различные рабочие места (РМ) относятся к той или иной категории по требуемой степени защищенности, и оформлять их в виде «Положения об определении требований по защите ресурсов»;
•***определять*** типовые конфигурации и настройки программно-аппаратных средств защиты информации для РМ различных категорий (требуемых степеней защищенности);
•по заявкам руководителей подразделений ***проводить анализ*** возможности решения (а также совмещения) указанных задач на конкретных РМ и принимать решения об отнесении РМ к той или иной группе по степени защищенности;
•совместно с ИТ - подразделением ***проводить работы*** по установке на РМ программно-аппаратных средств защиты информации;
•***согласовывать и утверждать*** предписания на эксплуатацию (формуляры) РМ, подготовленные в подразделениях организации;
•***обеспечивать*** проведение необходимых дополнительных специальных мероприятий по обеспечению безопасности информации;
•***определять организацию***, методики и средства контроля эффективности противодействия попыткам несанкционированного доступа к информации (НСД) и незаконного вмешательства в процесс функционирования автоматизированной системы.

ФУНКЦИИ ИТ – ОБЕСПЕЧЕНИЯ ПО РЕШЕНИЮ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИБ

проводить анализ возможности решения задач структурных подразделений на конкретных РМ и уточняет содержание необходимых для этого изменений в конфигурации аппаратных и программных средств РМ;
производить на основе утвержденных заявок начальников подразделений:
•установку (развертывание, обновление версий) программных средств;
•удаление (затирание) программ;
•установку (развертывание) новых РМ (ПК) или дополнительных устройств;
•изъятие или замену ПК;
•принимает участие в заполнении формуляров РМ и выдаче предписаний к эксплуатации РМ;

Служба ИТ (в части алгоритмов и программ) ***ведет*** общий перечень задач, решаемых в автоматизированной системе (АС) организации; совместно с подразделением ИБ ***оформляет*** формуляры установленного образца на новые функциональные задачи АС;
хранит установленным порядком и осуществляет резервное копирование и контроль целостности лицензионных дистрибутивов или эталонных носителей;
осуществляет выдачу специалистам службы ИТ программных пакетов для их развертывания или обновления на РМ АС

ФУНКЦИИ СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ КОМПАНИИ ПО ОБЕСПЕЧЕНИЮ ИБ

Определять функциональные задачи, которые должны решаться в подразделении с использованием РМ АС организации. Все необходимые изменения в конфигурации РМ и полномочиях пользователей подразделения осуществляют на основе заявок в соответствии с нормативными документами организации.

Заполнять формуляры РМ и представляют их на утверждение в подразделение ИБ.

Обеспечивать надлежащую эксплуатацию установленных на РМ средств защиты информации.




Квалифицированные специалисты

Мотивация

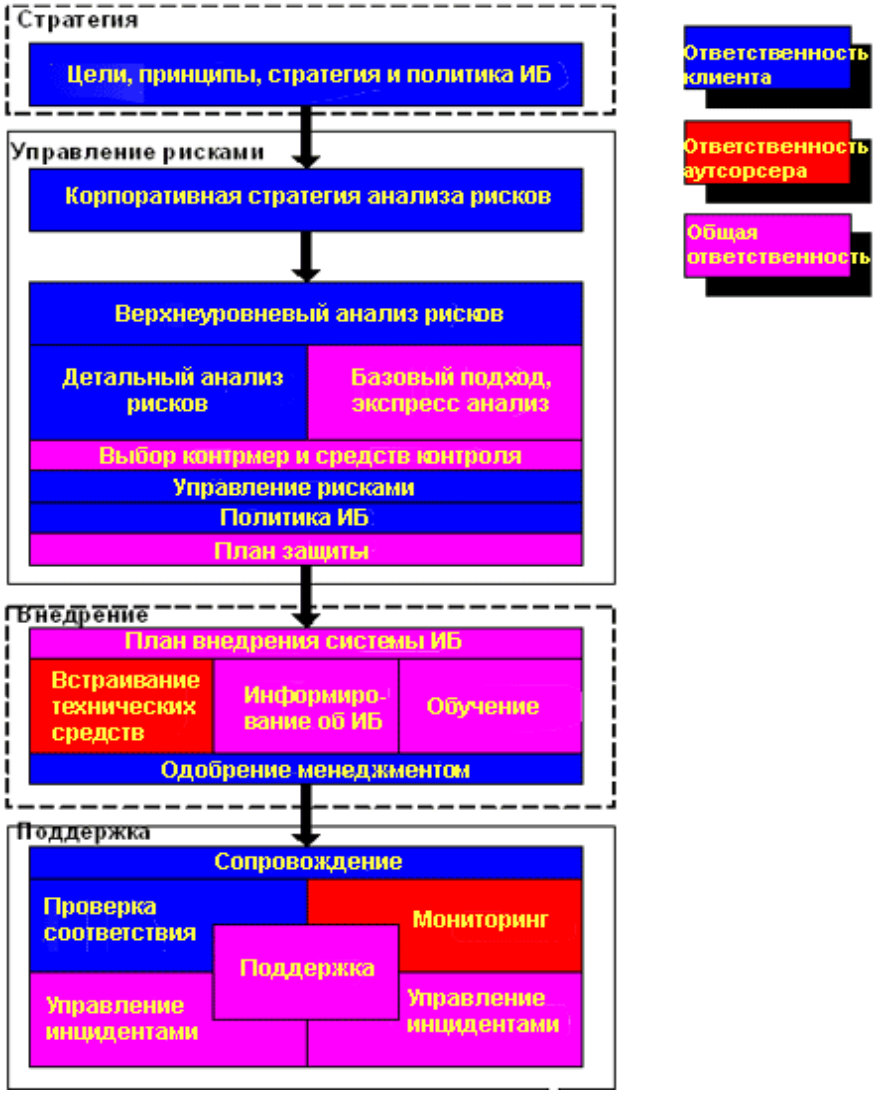
Аутсорсинг
Взаимодействие с государством

ПЕРСОНАЛ ПОДРАЗДЕЛЕНИЯ ИБ

Должен обладать:

a) надежностью и честностью;
b) ответственностью и объективностью;
c) знаниями, умениями и навыками в проверяемой области;
d) высшим профессиональным образованием;
e) работоспособностью и внимательностью;
f) способностями к выявлению новых угроз;
g) умением выделять главное;
h) умением четко излагать существо технической информации.

СООТНОШЕНИЕ СОБСТВЕННОЙ ДЕЯТЕЛЬНОСТИ И ИСПОЛЬЗОВАНИЕ УСЛУГ АУТСОРСИНГА.



ОСНОВНЫЕ ТРЕБОВАНИЯ К КОМПАНИИ-АУТСОРСЕРУ

1. Естественно, в первую очередь, это известное имя и хорошая репутация компании на рынке, большой опыт выполнения подобных проектов. Косвенно это свидетельствует о наличии достаточного штата высококвалифицированных сотрудников, необходимого программно-аппаратного обеспечения, налаженных связей с поставщиками решений.

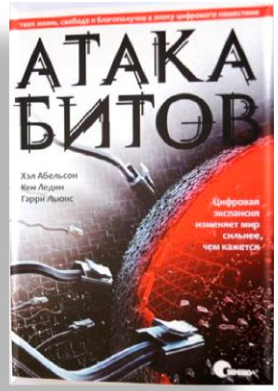
2. Аутсорсинговая компания должна иметь четкую и понятную политику ИБ, а также систему управления информационной безопасностью. В идеале – наличие сертификата ISO 27001.

3. Компания должна иметь опыт проведения анализа информационных рисков, практику управления рисками и соответствующие технические средства контроля.

4. Безусловно, требуется высокая профессиональная подготовка команды компании-аутсорсера, понимание проблем ИБ в той области бизнеса, в которой работает клиент.

5. Особое внимание следует уделить наличию средств контроля физической безопасности и технических средств контроля инженерных систем (систем кондиционирования, электропитания и др.).

6. Необходимо также определить систему и способ передачи данных между клиентом и аутсорсером.


АТАКА БИТОВ
Хэл Абельсон
Кен Леди
Гарри Льюис
Цифровая экспансия изменит мир сильнее, чем кажется


Национальная платежная система
Бизнес-энциклопедия


Безопасность карточного бизнеса
Бизнес-энциклопедия
МФПА
CompuTel
Золотая Корона


Обеспечение информационной безопасности бизнеса
под редакцией А.П. Курило
IBM
CompuTel


Д.А. Мельников
ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО - ТЕХНОЛОГИЧЕСКИХ СЕТЕЙ И СИСТЕМ
IDO PRESS


ВИКИ ЛИКС
КОМПРОМАТ НА РОССИЮ


Е. П. Ищенко
ВИРТУАЛЬНЫЙ КРИМИНАЛ


Юрий Жуков
ОСНОВЫ ВЕБ-ХАКИНГА
НАПАДЕНИЕ И ЗАЩИТА
DVD
ПИТЕР


ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
А. П. Курило
Н. Г. Милославская
М. Ю. Сенаторов
А. И. Толстой
ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ


ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
Н. Г. Милославская
М. Ю. Сенаторов
А. И. Толстой
УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ


Крис Просис
Кевин Мандиа
Расследование компьютерных преступлений


СЕРИЯ «ВЫСШАЯ ШКОЛА»
А.Ю. Щербаков
СОВРЕМЕННАЯ КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
Теоретические основы
Практические аспекты
Учебное пособие


В.А.Сердюк
ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ
ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ИНФОРМАЦИОННЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРЕДПРИЯТИЙ


Основы современной криптографии и стеганографии


Дж. Макнамара
СЕКРЕТЫ КОМПЬЮТЕРНОГО ШПИОНАЖА
ТАКТИКА И КОНТРМЕРЫ

Контрольные вопросы по 4-му разделу

1. Что такое промышленный шпионаж?
2. Каковы основные способы промышленного шпионажа?
3. Какие методы сбора разведданных используются в промышленном шпионаже?
4. Что понимается под оперативными видами разведки?
5. Какую роль играют технические средства промышленного шпионажа?
6. Что такое электронная разведка?
7. Чем можно объяснить дуализм отношений бизнеса и государства в сфере промышленного шпионажа?
8. Что вам известно о плане операции «Эшелон»?
9. Что такое информация ограниченного использования?
10. Какие существуют виды информации ограниченного использования?
11. Как осуществляется защита персональных данных?
12. Почему в отдельных случаях бизнес отвечает за защиту сведений, составляющих государственную тайну?
13. Что включает в себя система мер по защите конфиденциальной информации?
14. Кто и в каких случаях может получать информацию, составляющую банковскую тайну?
15. Какие меры предусмотрены нормативно-правовыми актами для защиты информации ограниченного использования?
16. Каким требованиям должна отвечать модель обеспечения кибернетической безопасности предприятия?
17. В чем заключается роль персонала в вопросах обеспечения кибернетической безопасности предприятия?
18. Каков механизм мошеннических действий по проникновению в систему банк-клиент?
19. Каковы основные методы расследования кибер-преступлений?
20. Что такое веб-хакинг и какой ущерб он может нанести предприятию?
21. В чем заключаются основы обеспечения сетевой безопасности?
22. Что такое фишинг, каковы основные меры противодействия?
23. Каковы основные правила обращения с носителями ЭЦП?