Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Семинар 3. Защита ноу-хау и коммерческой тайны при выполнении проектно-конструкторских работ

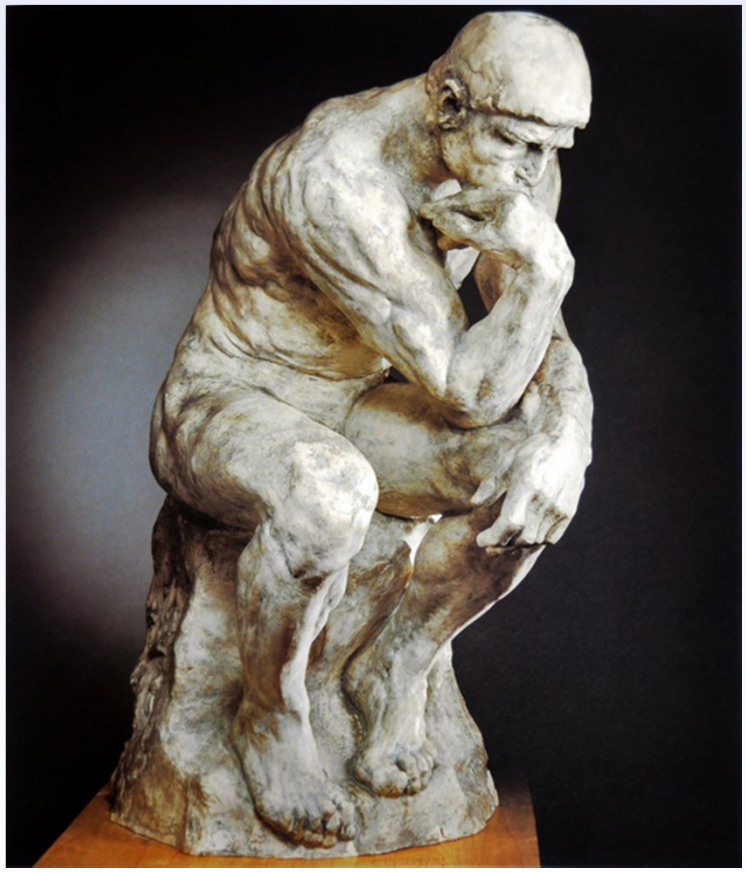
НТКС
Информационная безопасность

Форматы мероприятий для специалистов ИТ и ИБ.

Мероприятие / *Характеристика*	«Широко-форматная» конференция	Семинар одного вендора	Обучающие курсы "учебных центров"	Серия семинаров "ВЗЯТЬ ПОД КОНТРОЛЬ"
Многообразие тем	+	-	-	+
Время на раскрытие темы	-	+	+	+
Демонстрация продукта	-	+	-	+
Внутренняя логика и последовательность	-	+	+/-	+
Новый материал	+	+/-	+/-	+
Профессионализм докладчика	+/-	+	+/-	+
Общение участников	-	+/-	+	+
Выдача сертификата	-	-	+	+

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»



Задача серии семинаров:

обсудить и проработать практический состав **корпоративной системы обеспечения информационной безопасности**, последовательно разобрав ее основные аспекты и составные части.

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Ключевые особенности формата:

- последовательность и преемственность тематики семинаров,
- обсуждение теоретических и концептуальных моментов,
- изложение альтернативных подходов,
- полноценная демонстрация практических решений,
- формирование «клубного» общения.

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Ранее «пройденный» материал

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1. Понятие «безопасности».
2. Взаимосвязь задач бизнеса и задач ИБ.
3. «Непрерывный цикл» ИБ.

4. Элементы теории защиты информации.
5. Методы управления доступом (дискреционный, ролевой, мандатный).

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Ранее «пройденный» материал

ПРАКТИЧЕСКАЯ ЧАСТЬ (Управление доступом)

1. Контроль и аудит «матрицы доступа» к неструктурированным данным.
Varonis Data Governance Suite
2. Управление доступом на основе ролевой модели.
Программный комплекс **Avanpost. IDM+PKI+SSO**.
3. Управление классифицированными данными.
Реализация мандатная схемы в решении **Perimetrix**.

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Ранее «пройденный» материал

ПРАКТИЧЕСКАЯ ЧАСТЬ (Контроль действий пользователей)

4. Аудит, контроль и «видеозапись» действий пользователей. **ObserveIT**
5. Управление привилегированными учетными записями. **Enterprise Random Password Manager (Lieberman Software)**.

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Ранее «пройденный» материал

ДИСКУССИОННАЯ ЧАСТЬ

«ПРЕДОТВРАТИТЬ НЕЛЬЗЯ ПОЙМАТЬ».
Альтернативные подходы к борьбе с утечками важных данных.
Критический анализ классических DLP-решений.

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Краткое повторение пройденного

Безопасность – специфическая **совокупность условий** целенаправленной деятельности человека или организации, при которых эта деятельность достигает успеха.

То есть - совокупность условий, которые человек или организация усвоили, создали и могут контролировать.

Сформулированные топ-менеджментом «**условия безопасности бизнеса**» и приемлемые для организации **методы контроля** находят выражение в «Политике безопасности компании» и в ее частном проявлении – «Политике информационной безопасности».

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Краткое повторение пройденного

Корпоративная система менеджмента информационной безопасности –

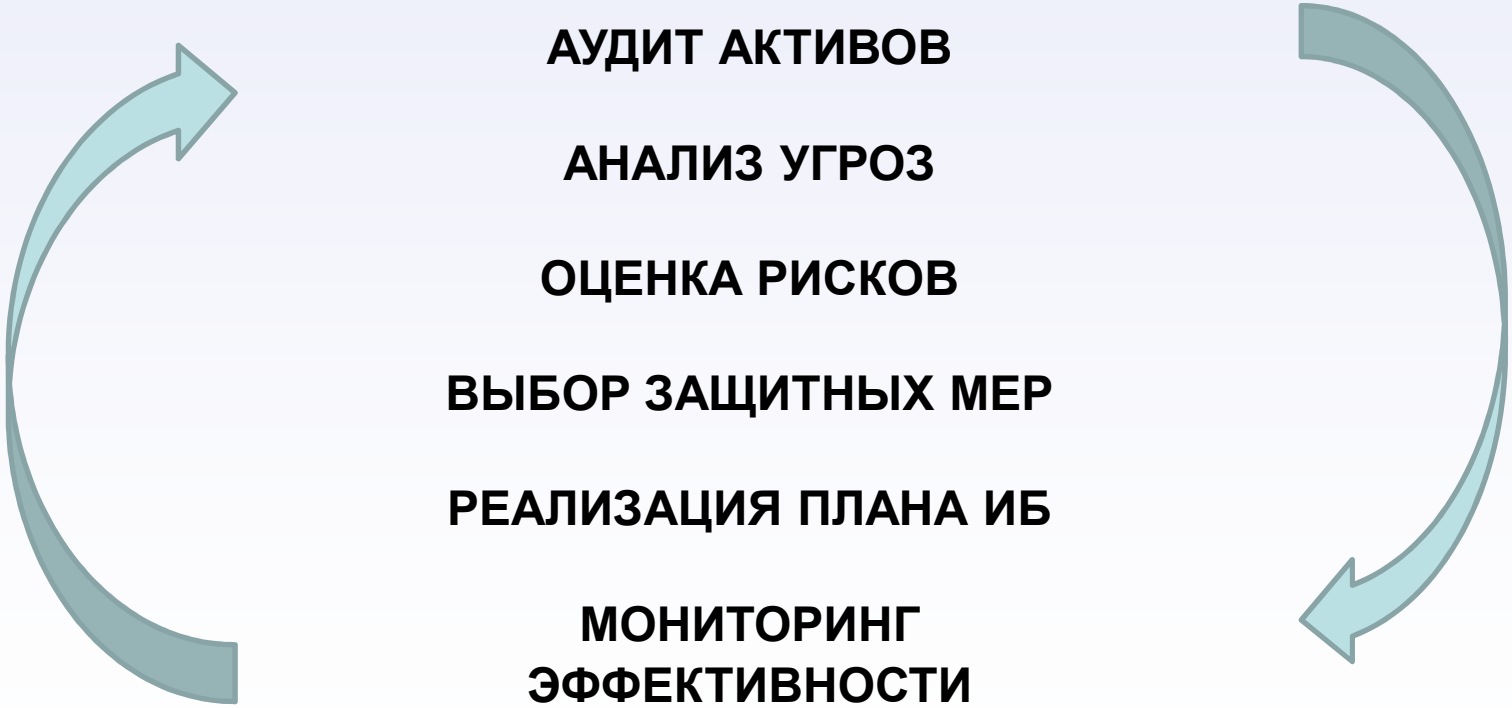
комплекс взглядов, подходов, организационных мер, технических средств и бизнес-процессов, предназначенных для обеспечения **безопасного, с точки зрения целей организации,** получения, хранения и обработки информации, циркулирующей как внутри самой организации, так и между организацией и окружающей ее средой.

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Краткое повторение пройденного

Непрерывный цикл управления ИБ



АУДИТ АКТИВОВ

АНАЛИЗ УГРОЗ

ОЦЕНКА РИСКОВ

ВЫБОР ЗАЩИТНЫХ МЕР

РЕАЛИЗАЦИЯ ПЛАНА ИБ

МОНИТОРИНГ ЭФФЕКТИВНОСТИ

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Краткое повторение пройденного

Элементы теории защиты информации:

Компьютерная система – совокупность
- объектов, содержащих информацию, и
- субъектов – особых объектов, способных выполнять преобразования объектов системы.

Субъект для выполнения преобразования использует информацию, содержащуюся в объектах компьютерной системы, т.е. осуществляет к ним доступ.

Основными видами доступа являются:
- доступ на чтение,
- доступ на запись,
- доступ на активизацию.

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Краткое повторение пройденного

Элементы теории защиты информации:

Основная аксиома защиты информации:

Все вопросы безопасности информации описываются доступами субъектов к объектам.

Практическое следствие:

Чтобы «ВЗЯТЬ ПОД КОНТРОЛЬ» информационную систему, первым делом необходимо отладить управление доступом к данным и другим ресурсам информационной системы.

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Краткое повторение пройденного

Дискреционное управление доступом (ACL, матрица доступа)

Субъект\Объект	Файл1	Файл2	Программа1	Программа 2
Пользователь 1	читать	читать, писать	запускать	
Пользователь 2	читать, писать		запускать	запускать
Пользователь 3	читать, писать	читать, писать		запускать
Пользователь 4	читать	читать	запускать	запускать
Программа 1	читать	писать		
Программа 2	читать			

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Краткое повторение пройденного

Управление доступом на основе ролей

Субъект\Объект	Файл1	Файл2	Программа1	Программа 2
Пользователь 1	читать	читать, писать	запускать	
Пользователь 2	читать, писать		запускать	запускать
Пользователь 3	читать, писать	читать, писать		запускать
Пользователь 4	читать	читать	запускать	запускать
Программа 1	читать	писать		
Программа 2	читать			

НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Краткое повторение пройденного

Мандатное (принудительное) управление доступом

разграничение доступа субъектов к объектам, основанное на назначении *метки конфиденциальности* для информации, содержащейся в объектах, и выдаче официальных разрешений (*мандатов допуска*) субъектам на обращение к информации такого уровня конфиденциальности.

Мандатное управление доступом сочетает защиту и ограничение прав, применяемых по отношению к компьютерным процессам, данным и системным устройствам и предназначено для предотвращения их нежелательного использования.

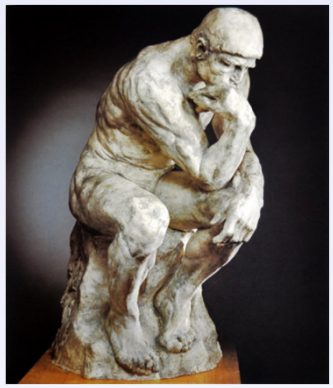
НТКС
Информационная безопасность

Серия семинаров «ВЗЯТЬ ПОД КОНТРОЛЬ»

Семинар 3. Защита ноу-хау и коммерческой тайны при выполнении проектно-конструкторских работ

НТКС
Информационная безопасность

Информация и информационные контейнеры



Мозг – первичный и наиболее важный, но не единственный контейнер для хранения информации.

Альтернативные контейнеры – книга, рисунок, видеозапись, чертеж, файл, вид из окна.

Перенос информации из контейнера в контейнер может сопровождаться невосстановимыми потерями.

Существуют несовместимые между собой виды информации, способы ее переноса и контейнеры для хранения.

НТКС
Информационная безопасность

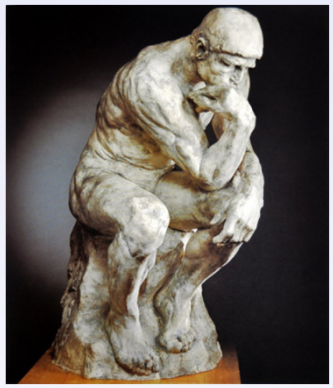
Информация и информационные контейнеры

Качество информации и возможность ее хранения, воспроизведения, дублирования и защиты впрямую зависят от используемого контейнера.

Выбор методов защиты информации зависит от возможных каналов воздействия на контейнер и возможных каналов (методов) передачи информации в другой контейнер.

НТКС
Информационная безопасность

Особенности современного «ноу-хау»

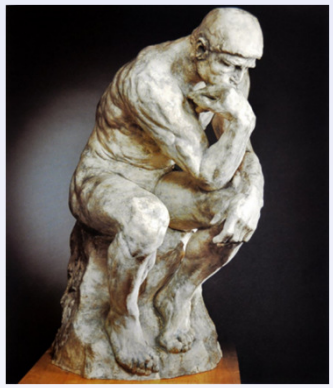


Современная информация класса «ноу-хау», как правило, представляет собой совокупность значительного числа информационных контейнеров, содержащих различные типы информации, создаваемой и обрабатываемой коллективно в процессе производственной деятельности.

Сложность и комплексность современного «ноу-хау» гарантирует невозможность его утраты/дублирования через примитивные каналы передачи информации (визуальный, слуховой, обонятельный и пр.).

НТКС
Информационная безопасность

Защита «ноу-хау» и проектно-конструкторской документации



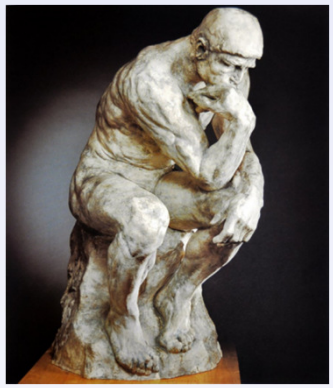
Число видов допустимых контейнеров для хранения частей «ноу-хау» и ПКД – ограничено.

Следовательно, ограничено и число вариантов воздействия на эти контейнеры и число возможных путей передачи информации в другие контейнеры.

Число же «допустимых» («разрешенных») путей еще меньше и может быть непротиворечиво описано в документах, регламентирующих соответствующие бизнес-процессы.

НТКС
Информационная безопасность

Защита «ноу-хау» и проектно-конструкторской документации



ОСНОВНОЙ МЕТОД:

Минимизация числа путей/способов передачи защищаемой информации из контейнера в контейнер выполняется по схеме:

«запрещено все, кроме того, что разрешено»,

а не по схеме
«разрешено все, кроме того, что запрещено».

Это и есть наиболее эффективная схема защиты.

НТКС
Информационная безопасность