ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Информационная безопасность в ВУЗе, ключевые направления

Власов Игорь Анатольевич
Начальник отдела информационной безопасности

Тольятти
2023

Организация обработки и защиты персональных данных

Специфика обработки ПДн

- Большое количество категорий ПДн
- Обработка ПДн студентов дистанционного обучения
- Обработка ПДн зарубежных студентов
- Обработка ПДн преподавателей из других регионов
- Передача сведений с ПДн во многие структуры
- **Управление согласиями на обработку и распространение ПДн**
- Большое количество запросов на передоставление ПДн от различных организаций

Специфика защиты ПДн

- Организация защиты ПДн при сравнительно небольшом бюджете
- Сайт Вуза с множеством поддоменов
- **Большое количество баз данных, содержащих ПДн**
- Программисты, системные администраторы с привелигированными правами
- Аутсорсинг поддержки ИСПДн
- Большое количество каналов возможной утечки ПДн
- Проблемы с кадровым обеспечением ОИБ

Что защищаем?
Как защищаем?

Определить активы

Выявить процессы

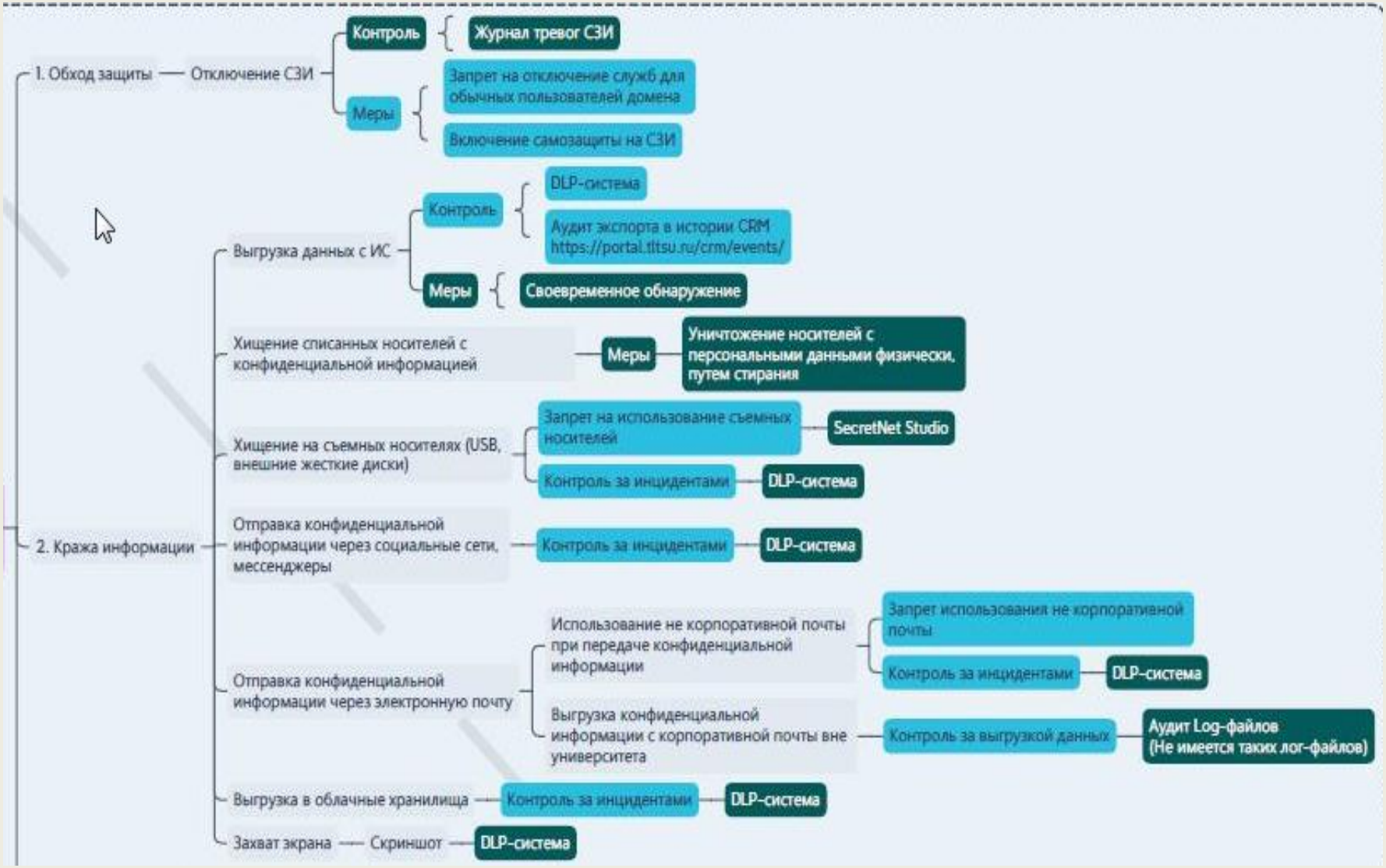
Откатегорировать процессы

Выявляем уязвимости

Активы + угрозы + уязвимости = риски

Определяем и реализуем защитные меры

Фрагмент реализации управления рисками



Обнаружение компьютерных атак и вторжений

Специфика целей

- получение контактных данных студентов
- экстремистский контент
- подмена информации
- закрепление в системе

Специфика принимаемых мер

- использование open source ПО
- ручной анализ логов доступа к КВО
- анализ трафика (NetFloor, WireShark...)
- анализ сайта и его поддоменов
- в плане IDS+TEAS

Проблемы

- бюджет на закупку NGFW, EDR, IDS+SIEM...и.т.д.
- компетенции сотрудников ОИБ
- удаленная техподдержка (атаки через них)

Управление доступом IDM

Специфика целей

- быстрая организация рабочего места
- прозрачность ролевой матрицы
- автоматизация распределения прав в большом количестве ИС

Специфика принимаемых мер

- вовлечение большого количества стейкхолдеров для описания процессов
- привлечение сторонних специалистов для внедрения

Проблемы

- большое количество не всегда согласованных процессов
- отсутствие бюджета на приобретение IDM

Управление уязвимостями

Специфика целей

- приоретизация уязвимостей к значимости бизнес - процессов и активов
- предотвращение утечек информации
- исполнение требований законодательства

Специфика принимаемых мер

- взаимодействие с ИТ - подразделениями для устранения выявленых уязвимостей
- использование специализированного ПО
- ручное выявление неправильной конфигурации сайтов (GIT репозитории, application.log...)

Проблемы

- сложности при взаимодействии с разработчиками сайтов
- сложности с устранениями уязвимостей на серверах, влекущих проблемы со связанным ПО

Защита данных

Специфика целей

- передача данных по защищенным каналам связи (VipNet Coord.\ Client)
- обмен трафиком между территориально удаленными объектами

Специфика принимаемых мер

- выделенная подсеть за МСЭ
- SecretNet с центром безопасности на ПК (защита от НСД)
- мониторинг активности
- разработана карта сети
- тестирование СЗИ от вендоров

Проблемы

-не всегда используется VPN
- сложности с устранениями уязвимостей на серверах, влекущих проблемы со связанным ПО

Управление электронными подписями

Специфика целей

- контроль всех бизнес-процессов, связанных с ЭП
- централизация учета СКЗИ
- оперативность устранения проблем

Специфика принимаемых мер

- централизация оформления ЭП и взаимодействия с УЦ
- оперативное реагирование на изменение законодательства
- повышение осведомленности пользователей

Проблемы

- обучение сотрудников ИБ управлению ЭП
- «зоопарк» ПО при использовании ЭП, настройке доступа, администрированию

Управление компьютерными инцидентами

Специфика целей

- оперативное выявление КИ, реагирование, нейтрализация последствий
- оперативное взаимодействие с НКЦКИ, регуляторами

Специфика принимаемых мер

- разработка вменяемых, актуализируемых регламентов по выявлению КИ и оперативному реагированию
- тренинги оперативных групп
- разбор КИ с участием руководства и заинтересованных стейкхолдеров

Проблемы

- слабые компетенции сотрудников ОИБ
- разработка плейбуков

Предотвращение и обнаружение утечек информации

Специфика целей

- оперативное выявление факта утечки, реагирование, нейтрализация последствий
- оперативное взаимодействие с регуляторами по факту утечки ПДн

Специфика принимаемых мер

- использование DLP
- оперативная работа с пользователями по вывлению каналов утечек
- контроль исходящего трафика

Проблемы

- отсутствие возможности контроля удаленной работы (VDI есть, модуля контроля нет)
- отсутствие контроля привелигированных пользователей

Повышение осведомленности пользователей

Специфика целей

- доведение требований ИБ, повышение осведомленности в вопросах ИБ большого количества пользователей

Специфика принимаемых мер

- оперативное информировние о наиболее значимых требований ИБ и контроль их исполнения
- проведение фишинговых учений

Проблемы

- отсутствие общедоступного медийного ресурса для размещения ИБшных страничек

КИИ

Специфика целей	-учет объектов КИИ по разделу научная деятельность
Специфика принимаемых мер	- выявление критически значимых процессов при слабом вовлечении сотрудников, занятых научной деятельностью
Проблемы	- отсутствие специалиста КИИ

Спасибо за внимание!