

Управление образования и науки Липецкой области
Государственное областное бюджетное
профессиональное образовательное учреждение
«Лебедянский торгово-экономический техникум»

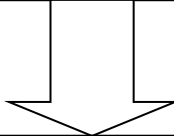
Выпускная квалификационная работа

**Тема: «Оценка защиты web-ресурсов от
кибератак»**

**Подготовил
Пургин М. А.
Руководитель
Зеленева Т. А.**

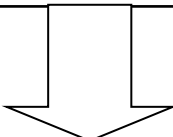
СИСТЕМНАЯ МОДЕЛЬ ИССЛЕДОВАНИЯ

ТЕМА: «Оценка защиты web-ресурсов от кибератак»



ОБЪЕКТ ИССЛЕДОВАНИЯ – система информационной безопасности и меры защиты корпоративной информации ОБУ «ЦСЗН по Данковскому району».

ПРЕДМЕТ ИССЛЕДОВАНИЯ – оценка уровня кибербезопасности web-ресурсов ОБУ «ЦСЗН по Данковскому району»

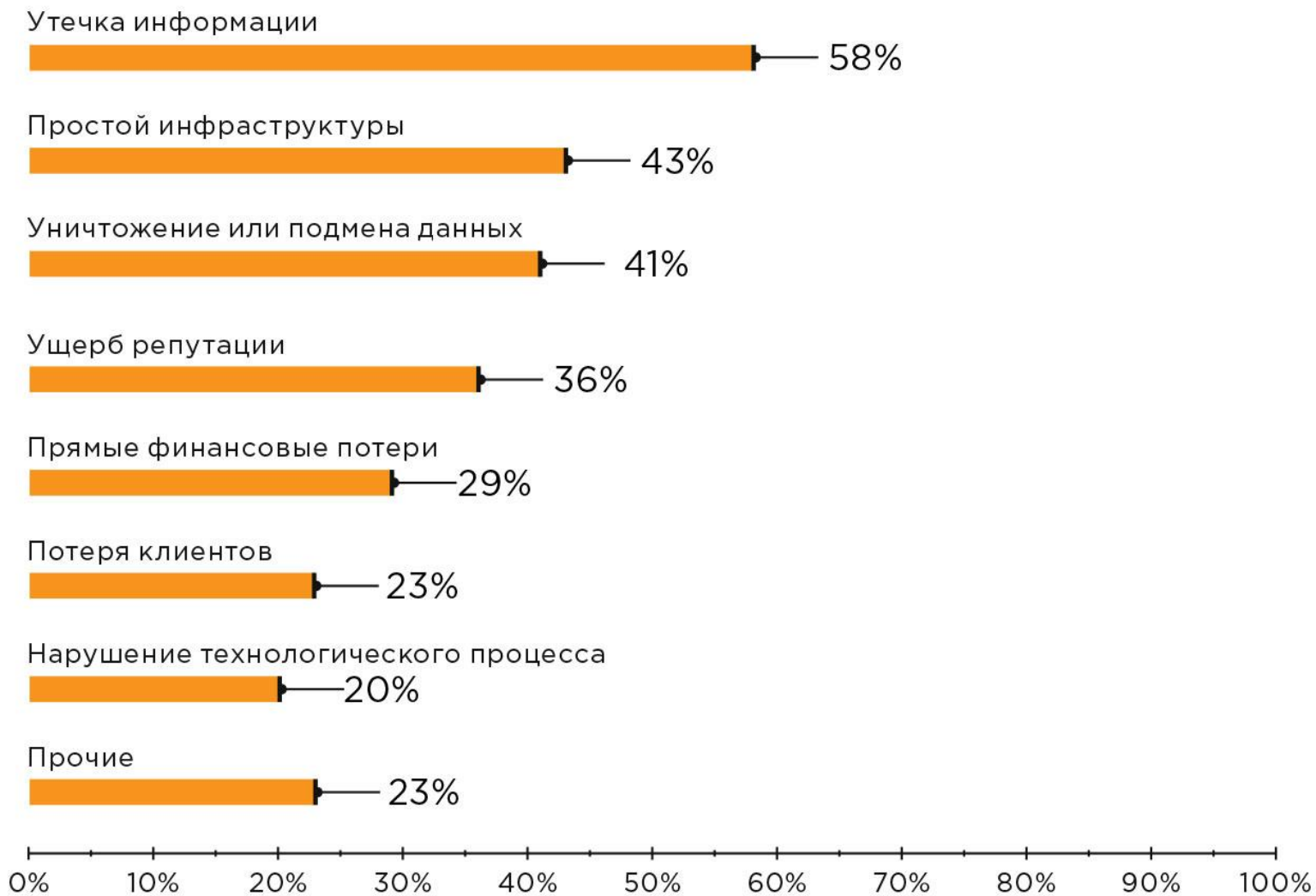


ЦЕЛЬ ИССЛЕДОВАНИЯ – мониторинг уровня защищенности информационной системы ОБУ «ЦСЗН по Данковскому району» от кибератак и выработка рекомендаций по ее повышению в отношении актуальных угроз кибербезопасности.

ЗАДАЧИ ИССЛЕДОВАНИЯ:

- проведение анализа угроз кибербезопасности и уязвимости информационной системы организации;
- выявление объектов информационной безопасности и недостатков в системе защиты web-ресурсов;
- описание мер, методов, средств защиты информации, наиболее реальных угроз;
- изучение методики проведения оценки безопасности web-ресурсов;
- проведение тестирования системы на устойчивость к кибератакам;
- выработка комплекса мероприятий, направленных на повышение уровня защищенности корпоративной информации.

С какими последствиями кибератак сталкивались компании



Меры, направленные на:

**обеспечение защиты информации от
неправомерного доступа, уничтожения,
модифицирования, блокирования, копирования,
предоставления, распространения, а также от
иных неправомерных действий в отношении
такой информации**

**соблюдение конфиденциальности
информации ограниченного доступа**

реализацию права на доступ к информации

Актуальные векторы атак



■ Угрозы, связанные с персоналом

■ Угрозы, связанные с эксплуатацией уязвимостей

■ Использование закладок

Нормативные требования по защите персональных данных (ПДн)

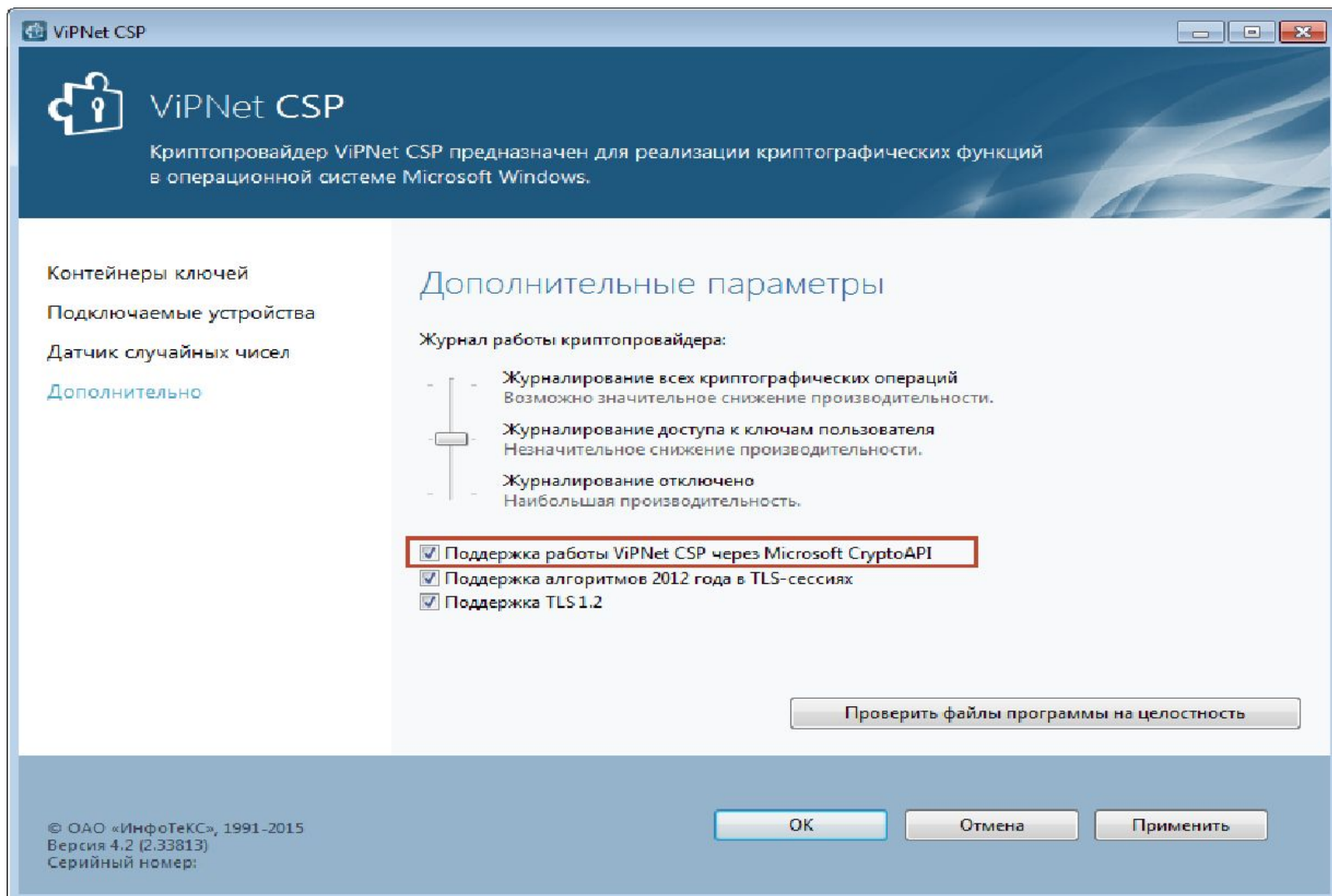
Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»:


- ✓ определяет Меры по обеспечению безопасности персональных данных при их обработке (статья 19)
- ✓ устанавливает, что требования по обеспечению безопасности ПДн распространяются на все организации, которые осуществляют обработку ПДн
- ✓ определяет, что требования по обеспечению безопасности ПДн, устанавливаются ФСТЭК России и ФСБ России в пределах их полномочий

Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Программа ViPNet CSP





В 2019 расходы из-за киберпреступности увеличились на 23 % в сравнении с 2018 годом.

В среднем эта сумма составляет 11,7 миллионов долларов.

Средняя сумма убытков компании, вызванных атакой вредоносной программы, составляет 2,4 миллиона долларов.

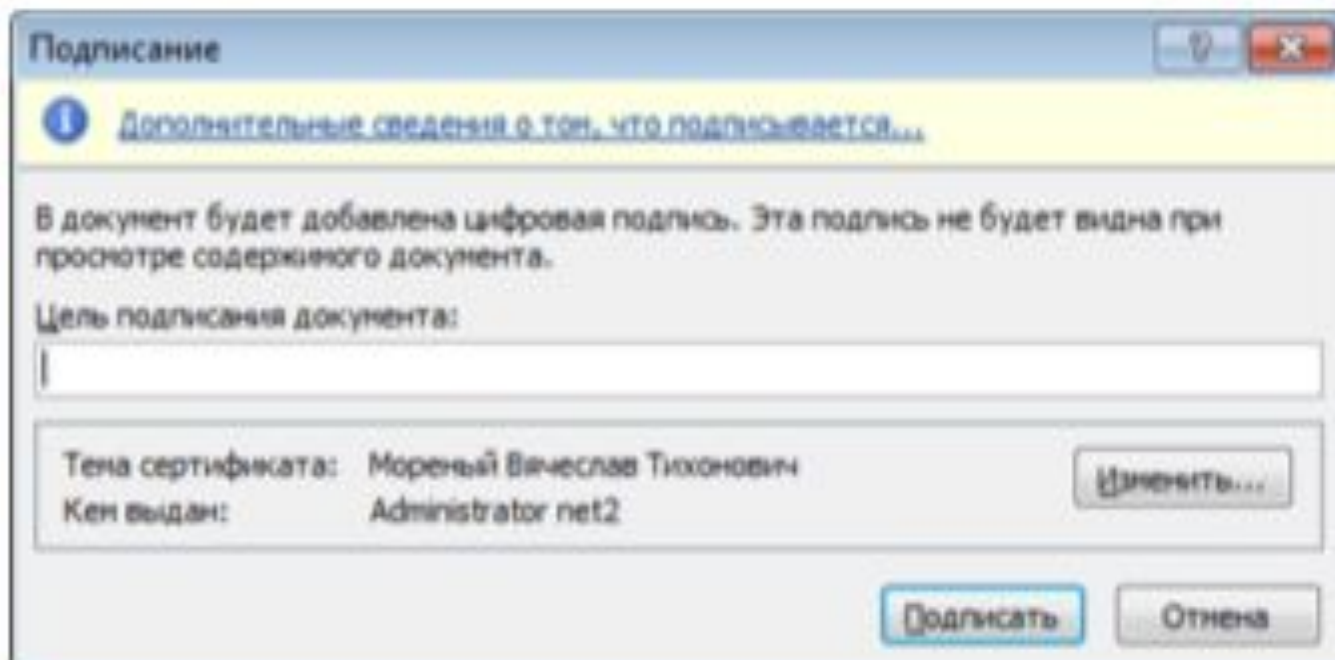
С 2018 по 2019 год расходы на кибербезопасность выросли на 22,7 %.

Средняя сумма ущерба от киберпреступности по всему миру выросла более чем на 27 %.

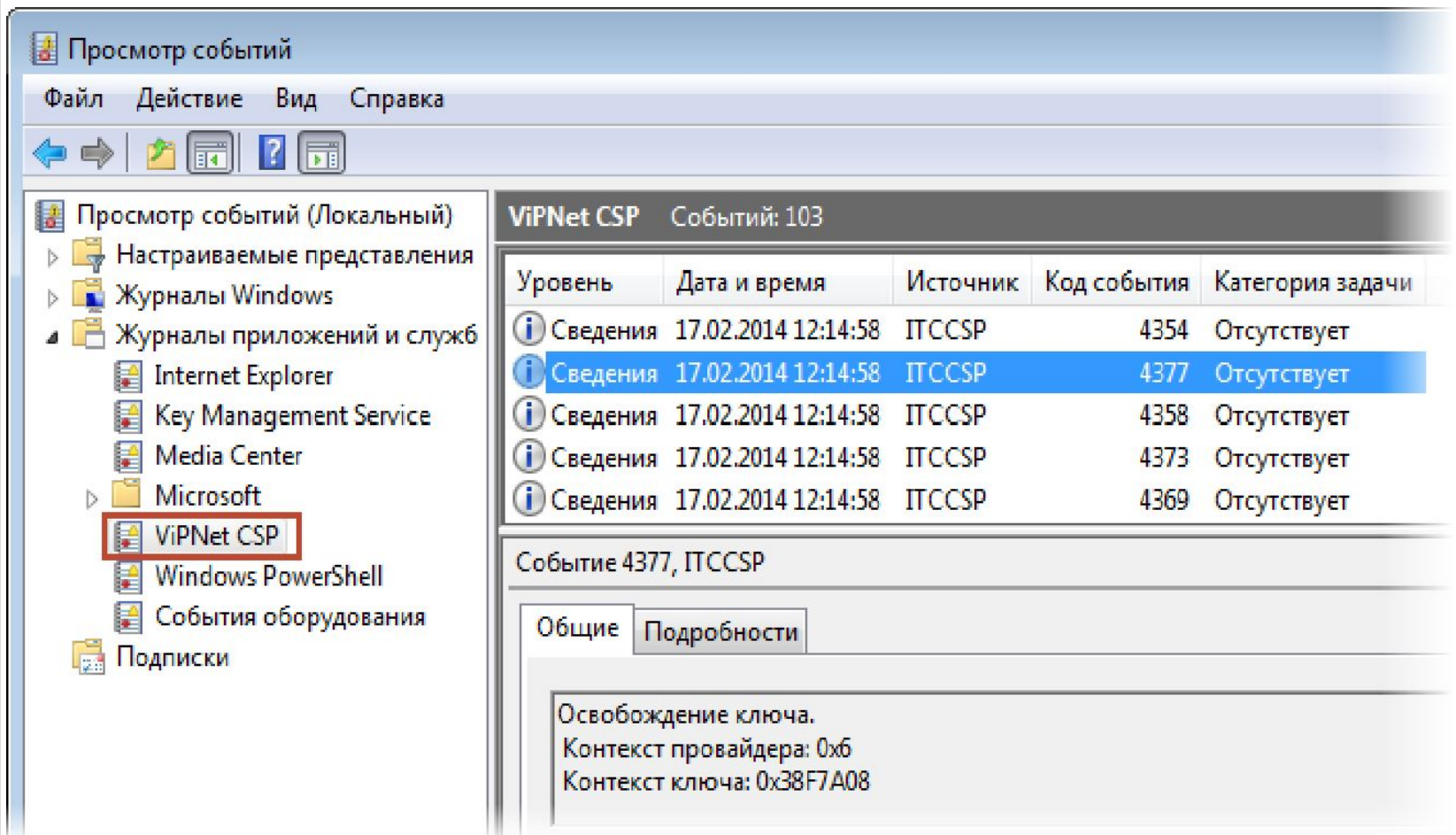
Самый дорогой аспект кибератаки для предприятий — потеря информации.

Она составляет 43 % всех затрат, вызванных вторжениями злоумышленников.

Добавление электронной ПОДПИСИ



Просмотр событий ViPNet CSP



The screenshot shows the Windows Event Viewer application. The left pane displays the event log tree with 'ViPNet CSP' selected under 'Журналы приложений и служб'. The right pane shows a list of 103 events for ViPNet CSP, with event 4377 highlighted. Below the list, the details for event 4377 are shown, including the message 'Освобождение ключа' and context information.

Просмотр событий

Файл Действие Вид Справка

Просмотр событий (Локальный)

- Настраиваемые представления
- Журналы Windows
- Журналы приложений и служб
 - Internet Explorer
 - Key Management Service
 - Media Center
 - Microsoft
 - ViPNet CSP**
 - Windows PowerShell
 - События оборудования
 - Подписки

ViPNet CSP Событий: 103

Уровень	Дата и время	Источник	Код события	Категория задачи
Сведения	17.02.2014 12:14:58	ITCCSP	4354	Отсутствует
Сведения	17.02.2014 12:14:58	ITCCSP	4377	Отсутствует
Сведения	17.02.2014 12:14:58	ITCCSP	4358	Отсутствует
Сведения	17.02.2014 12:14:58	ITCCSP	4373	Отсутствует
Сведения	17.02.2014 12:14:58	ITCCSP	4369	Отсутствует

Событие 4377, ITCCSP

Общие Подробности

Освобождение ключа.
Контекст провайдера: 0x6
Контекст ключа: 0x38F7A08

Рекомендации

Обязательное применение новейших средств антивирусной защиты. Важно сейчас использование многоуровневой антивирусной защиты, использование комплекса антивирусного ПО.

Продукт от «Лаборатории Касперского» KIS 2011 является сейчас самым оптимальным средством защиты не только от вирусов, но и от целого ряда других угроз безопасности информации.

Резервное копирование в онлайн-хранилищах. Поместить данные в одну из современных «облачных» служб.

ВЫВОД

Для обеспечения безопасности в ИС необходимо учитывать не только основные принципы обеспечения информационной безопасности, но и применять постоянно совершенствующиеся методы и способы защиты.

С учетом многих параметров защищаемой сети, особенностей организации, характера ее деятельности и бюджета должна быть создана конкретная политика обеспечения информационной безопасности.

Необходимо постоянно учитывать новые угрозы, обновлять программный и аппаратный комплекс средств защиты.

Построение грамотной методики обеспечения информационной безопасности в каждом конкретном случае, с учетом всех внутренних и внешних факторов позволит создать действительно эффективную систему информационной безопасности, обеспечивая достаточный уровень защиты.



**Спасибо
за внимание!**