СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

СибГУТИ

Программно-аппаратные средства обеспечения информационной безопасности

к.т.н., доцент кафедры
«Безопасность информации
и технологий» (БИТ)
Солонская Оксана Игоревна
https://vk.com/ok_solonskaya
solonskaya@sibguti.ru

Занятия по дисциплине

Лекционные – 2 часа занятий каждую неделю до перелома, после – раз в две недели.

Лабораторные – 2 часа занятий в неделю.

Практические – 2 часа занятий раз в две недели.

Экзамен.

Курсовой проект:

- выдача задания – 9 неделя;
- досрочная сдача – 13 неделя;
- в срок – 14 неделя.

Все материалы будут доступны в **ЭИОС** зарегистрированным пользователям:
https://eios.sibsutis.ru/course/view.php?id=844

Список основной литературы

1. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87992.html (дата обращения: 04.09.2022). — Режим доступа: для авторизир. пользователей
2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 04.09.2022). — Режим доступа: для авторизир. пользователей
3. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — Самара : Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — ISBN 978-5-9585-0603-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/43183.html (дата обращения: 04.09.2022). — Режим доступа: для авторизир. пользователей

Список дополнительной литературы

1. Построение коммутируемых компьютерных сетей : учебное пособие / Е. В. Смирнова, И. В. Баскаков, А. В. Пролетарский, Р. А. Федотов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 428 с. — ISBN 978-5-4497-0350-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89464.html (дата обращения: 04.09.2022). — Режим доступа: для авторизир. пользователей

СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

СибГУТИ

1 Основные термины и определения

Информация – сведения (сообщения, данные) независимо от формы их представления. [ФЗ №149]

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. [ГОСТ Р 50922-2006]

Безопасность информации (данных)– состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность. [ГОСТ Р 50922-2006]

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии.

Основные характеристики информации [Р 50.1.053-2005]

Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на это право.

Целостность – состояние информации, при котором ее изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Доступность – состояние информации, при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно.

Классификация информации по степени конфиденциальности

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. [ФЗ № 149]

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [ФЗ № 149]

Система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации. [ГОСТ Р 50922-2006]

Компоненты информационной системы

аппаратные средства

программные средства

данные

персонал

в терминологии систем управлении доступа

объекты системы

субъекты системы

Уязвимость информационной системы – свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации. [ГОСТ Р 50922-2006]

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. [ГОСТ Р 50922-2006]

Атака – действия, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы с применением программных и (или) технических средств. [Р 50.1.056-2005]

Примечание: условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в информационной системе. Если уязвимость соответствует угрозе, то существует риск.

Несанкционированный доступ – доступ к информации (ресурсам автоматизированной информационной системы), осуществляемый с нарушением установленных прав и (или) правил доступа к информации (ресурсам автоматизированной информационной системы). [Р 50.1.056-2005]

Несанкционированное воздействие на информацию – изменение информации (ресурсов автоматизированной информационной системы), осуществляемое с нарушением установленных прав и (или) правил. [Р 50.1.056-2005]

Примечания: НСД и НСВ может быть осуществлено преднамеренно или непреднамеренно.

Органы, осуществляющие контроль и регулирование в области информационной безопасности

Федеральная служба по техническому и экспортному контролю (**ФСТЭК России**)

ФСБ России

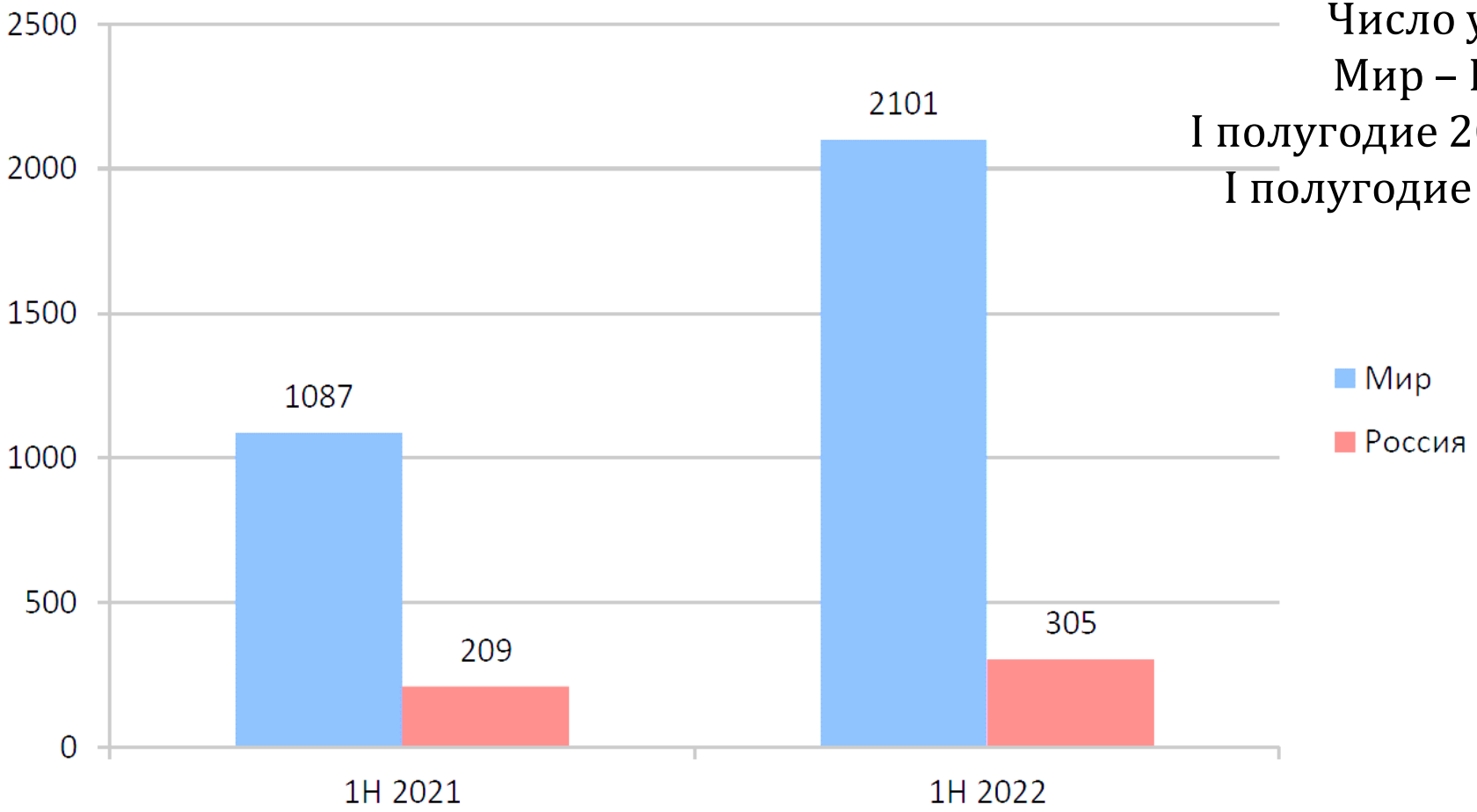
Министерство цифрового развития, связи и массовых коммуникаций РФ (**Минкомсвязь России**)

Федеральное агентство по техническому регулированию и метрологии (**Росстандарт**)

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (**Роскомнадзор**)

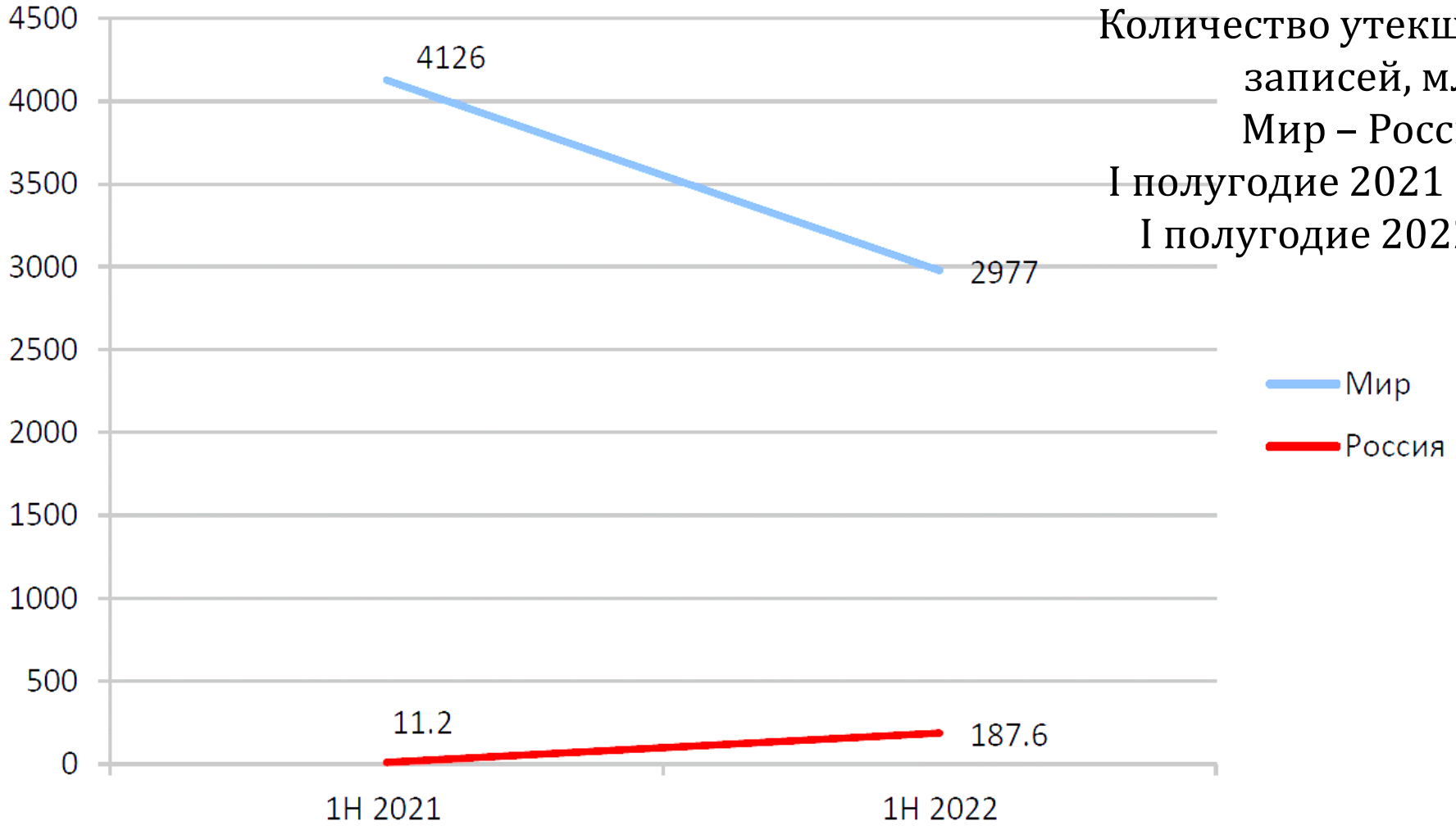
Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года

Число утечек:
Мир – Россия,
I полугодие 2021 г. –
I полугодие 2022 г.

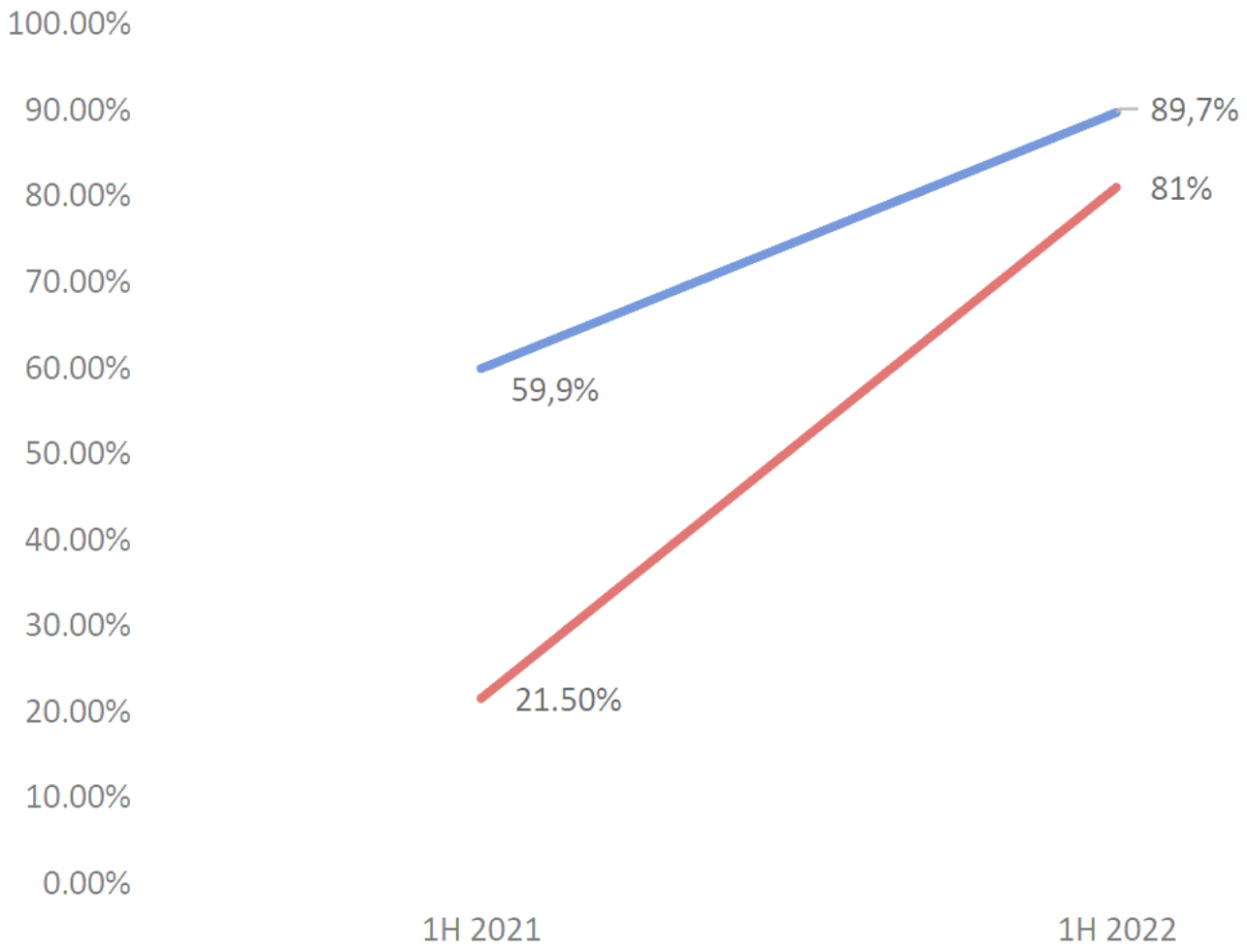


Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года

Количество утекших записей, млн:
Мир – Россия,
I полугодие 2021 г. –
I полугодие 2022 г.



Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года



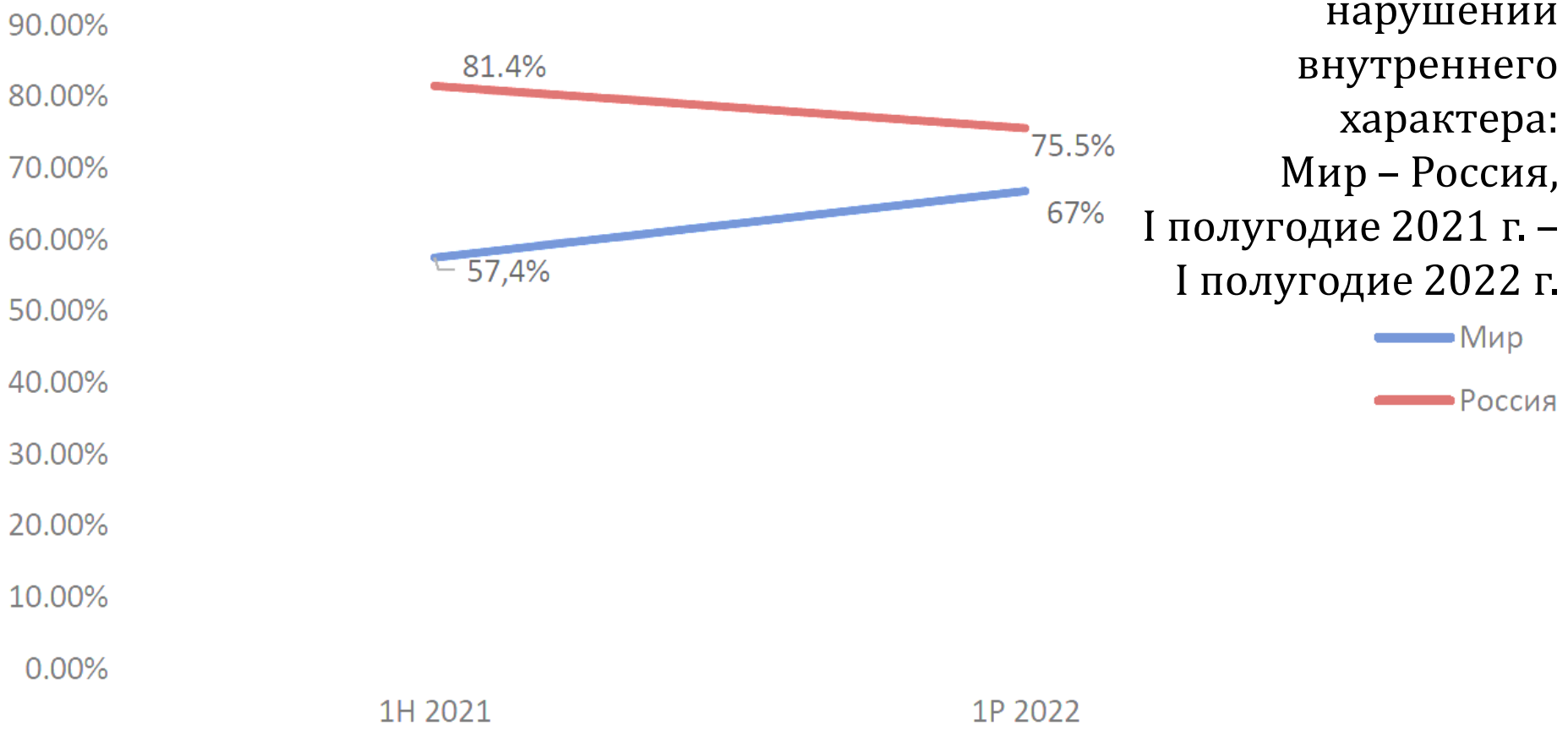
Динамика доли утечек вследствие внешнего воздействия: Мир – Россия, I полугодие 2021 г. – I полугодие 2022 г.

Мир

Россия

Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года

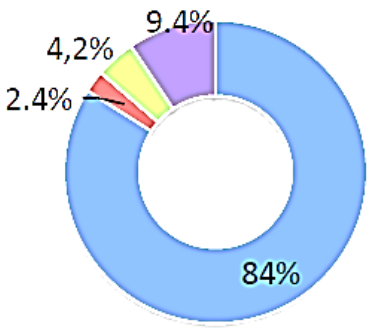
Доля умышленных нарушений внутреннего характера: Мир – Россия, I полугодие 2021 г. – I полугодие 2022 г.



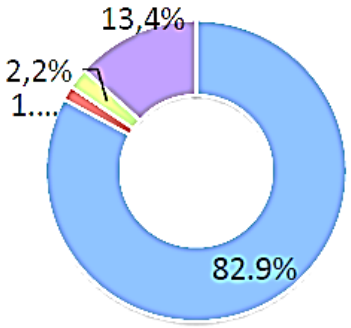
Новосибирск, 2023

Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года

Мир 1H 2021

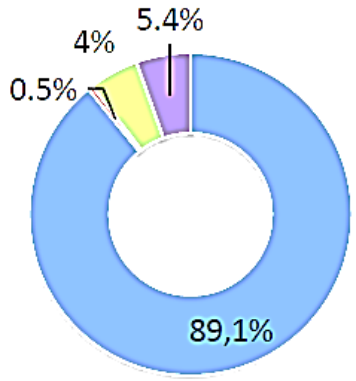


Мир 1H 2022

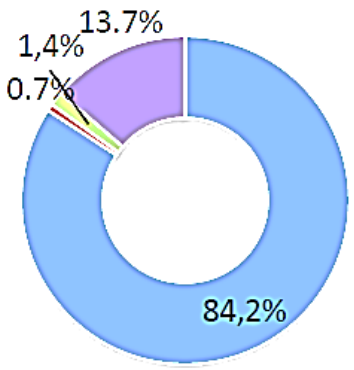


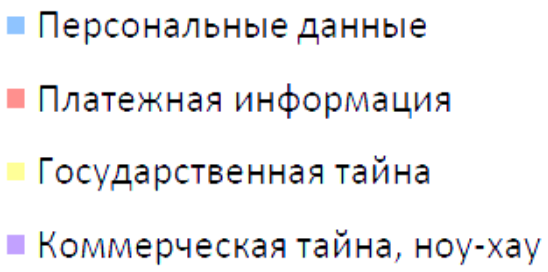
Распределение утечек по типам данных:
Мир - Россия,
I полугодие 2021 г. –
I полугодие 2022 г.

Россия 1H 2021



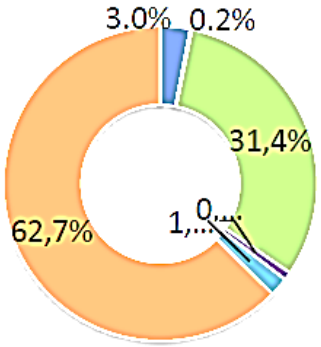
Россия 1H 2022



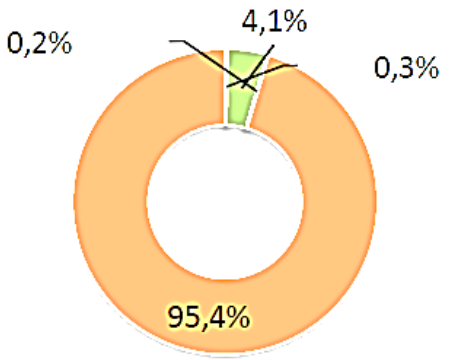


Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года

Мир 1H 2021

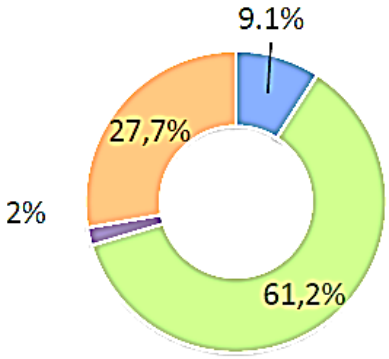


Мир 1H 2022

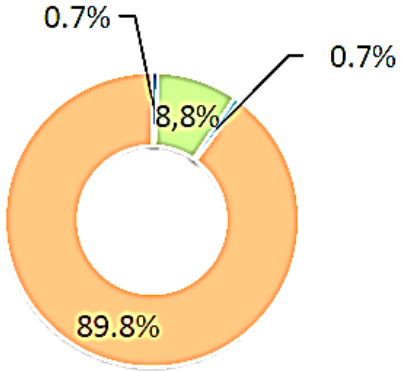


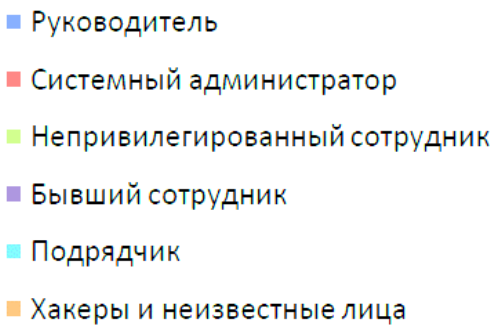
Распределение утечек по виновникам: Мир – Россия, I полугодие 2021 г. – I полугодие 2022 г.

Россия 1H 2021



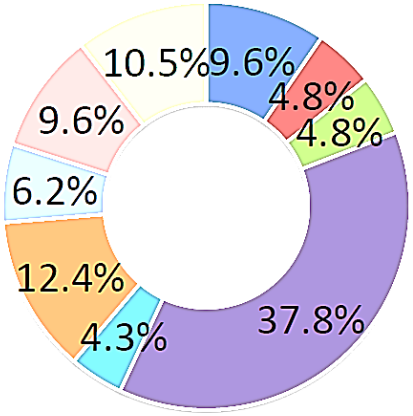
Россия 1H 2022



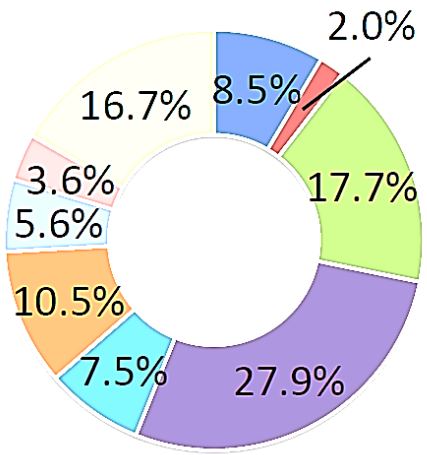


Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года

Россия 1H 2021



Россия 1H 2022

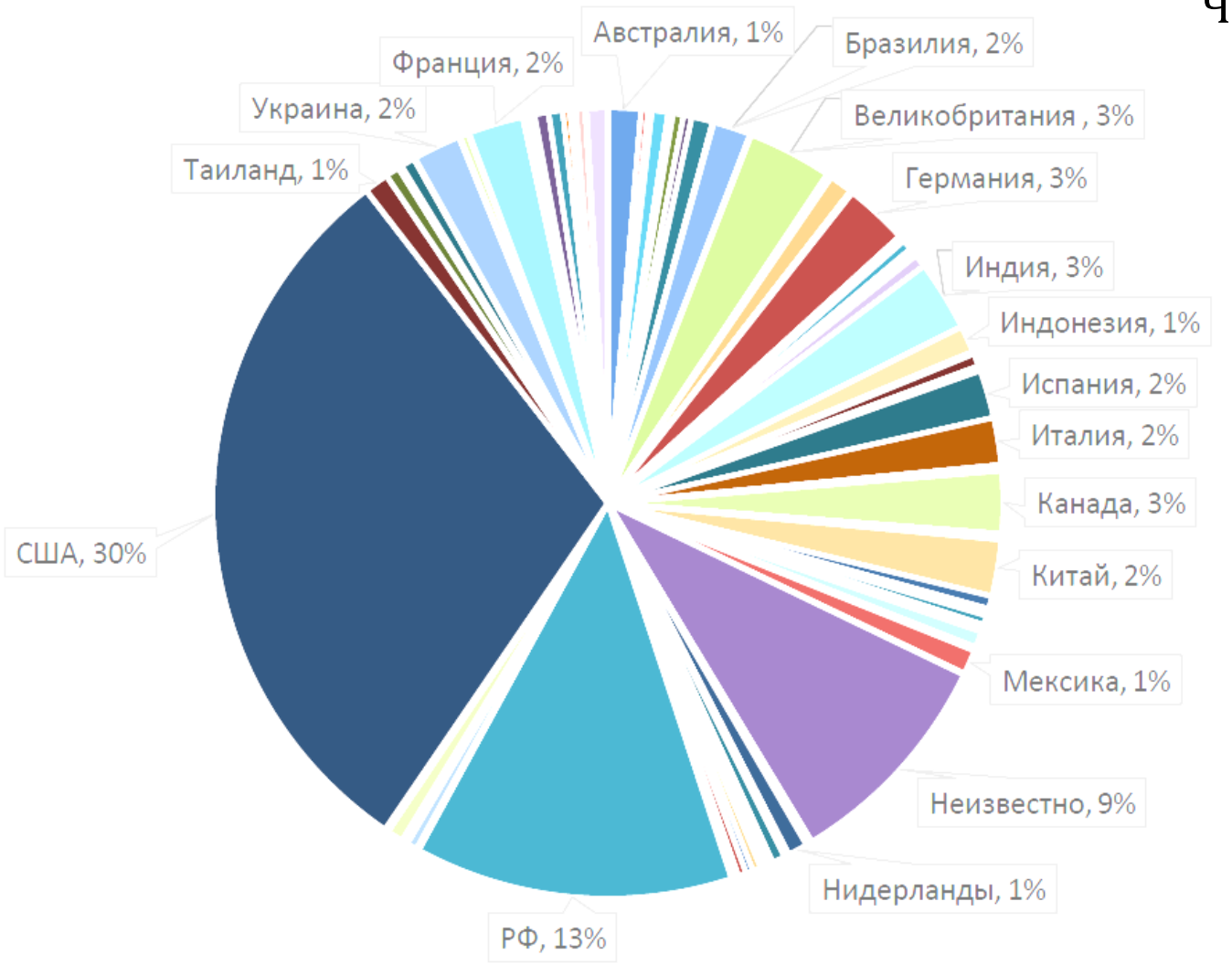


Отраслевое распределение утечек, Мир – Россия, I полугодие 2021 г. – I полугодие 2022 г.

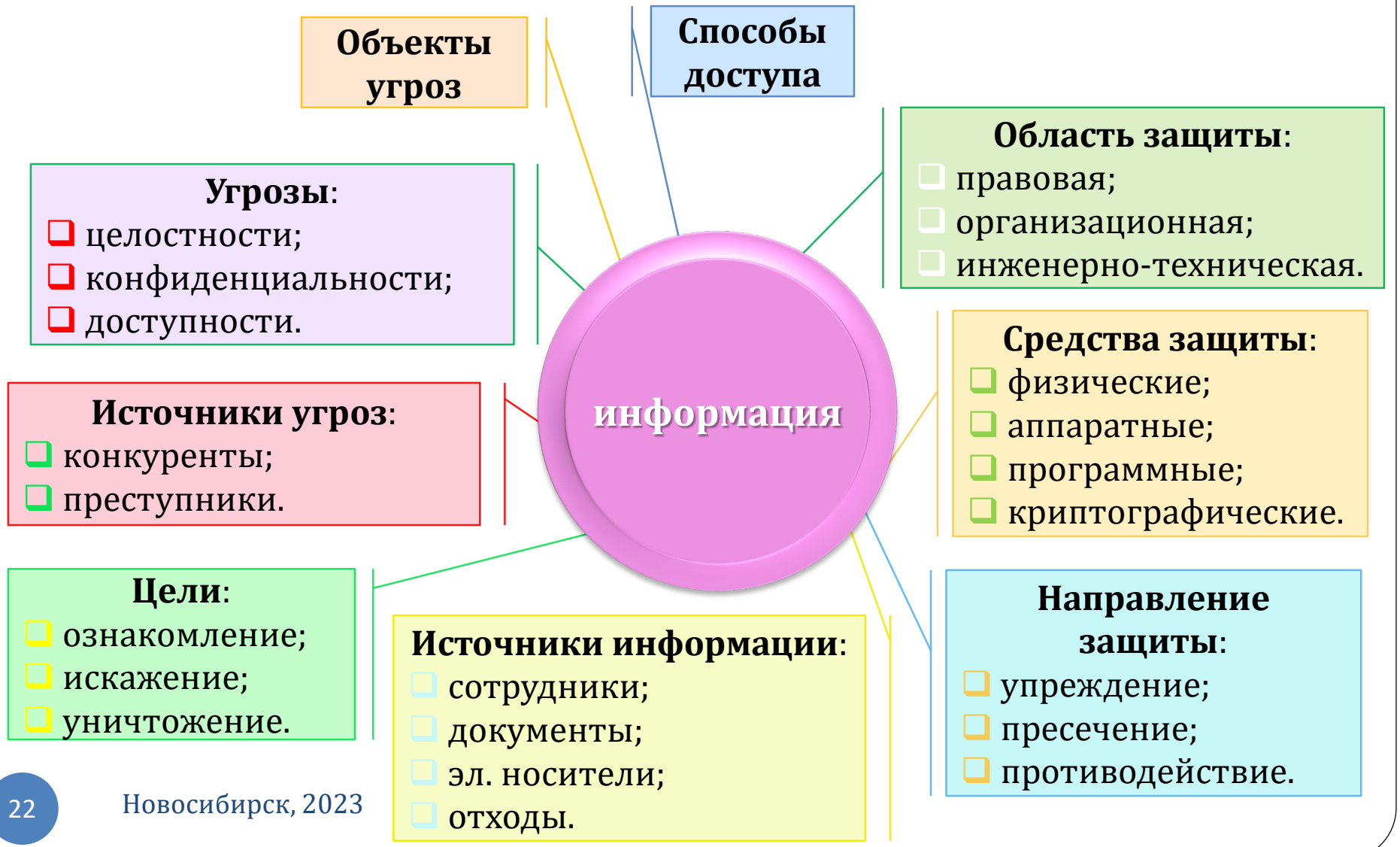
- Банки и финансы
- Здравоохранение
- Торговля, HoReCa
- Высокие технологии
- Промышленность и транспорт
- Госорганы и силовые структуры
- Образование
- Муниципальные учреждения
- Другое/не определено

Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года

Число объявлений о продаже данных



Модель защиты информации



Новосибирск, 2023

СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

СибГУТИ

2 Аутентификация пользователей информационных систем