Код безопасности

Защита информации на рабочих станциях и серверах

Аналитическое исследование
Декабрь 2016 г.

Содержание

Резюме

По итогам исследования аналитиками «Кода безопасности» были сделаны следующие выводы:

34% актуальных угроз безопасности информации на рабочих станциях и серверах составляют **угрозы несанкционированного доступа**.

ТОП-5 угроз безопасности: неправомерное ознакомление с защищаемой информацией **(79%)**, несанкционированная модификация защищаемой информации **(77%)**, распространение «почтовых червей» **(76%)**, утрата носителей информации **(72%)**, кража учетной записи доступа к сетевым сервисам **(66%)**.

В среднем по рынку для обеспечения безопасности **1** компьютера используются **3** средства защиты. В банковском и телеком-сегментах обычно используют сразу **6 СЗИ**.

В каждой **5-й** компании персональные данные обрабатываются только на **1** компьютере.

В **31%** организаций за защиту информации отвечают **НЕ** ИБ-специалисты.

47% информационных систем персональных данных являются специальными.

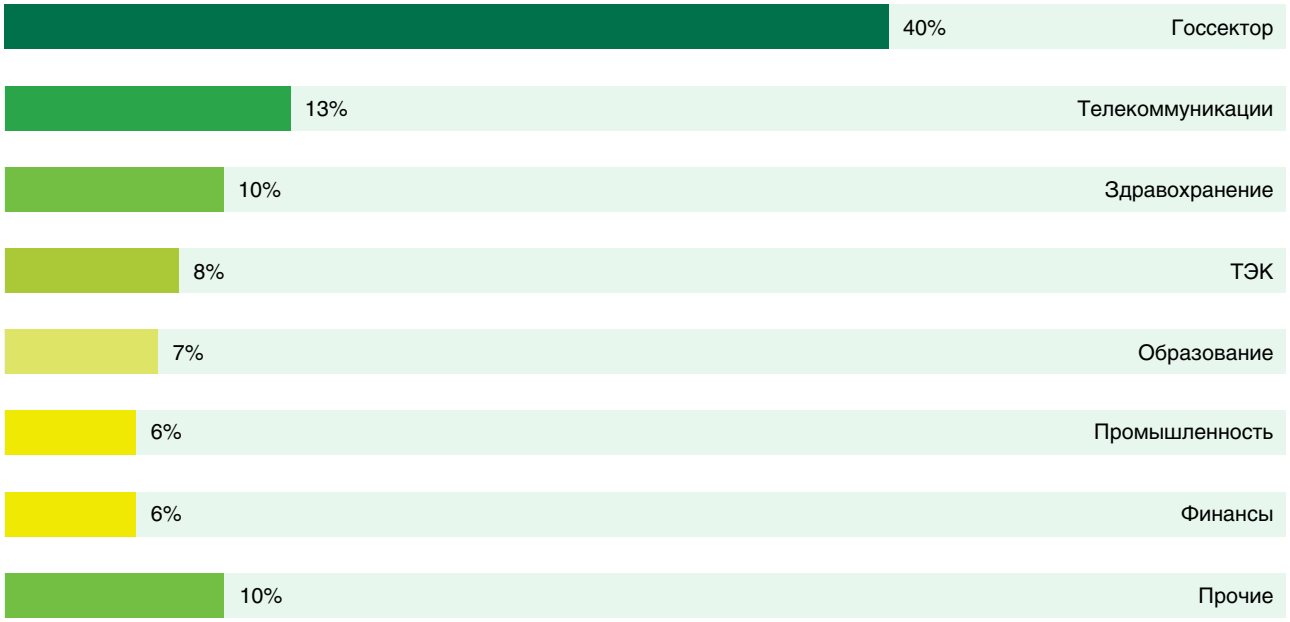
53% ИБ-бюджета тратят компании на защиту рабочих станций, серверов и сетевого взаимодействия.

Методика сбора данных и анализа

Опрос проводился онлайн на сайте компании «Код безопасности». В основе результатов, рассматриваемых в данном исследовании, лежат ответы более 500 респондентов из 11 отраслей. Это сотрудники следующих категорий: руководители компаний, директора по информационной безопасности, директора по информационным технологиям, руководители служб безопасности, ИТ- и ИБ-специалисты.

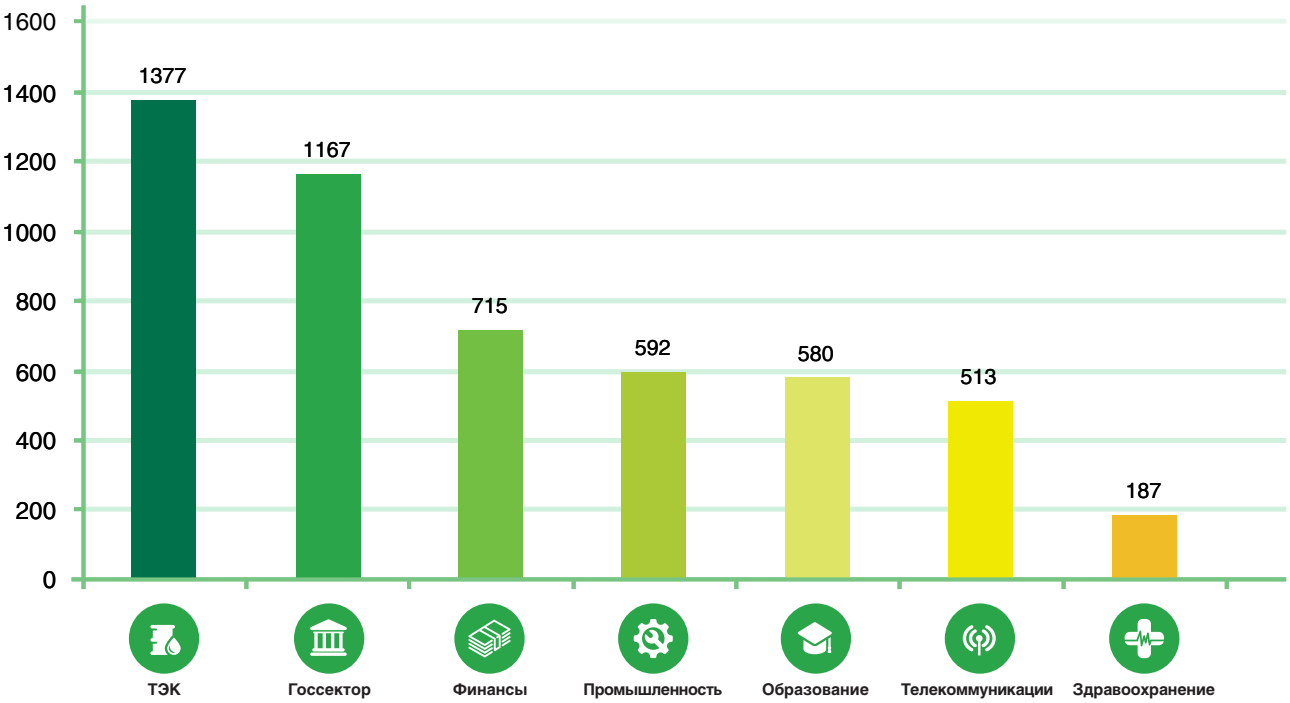
В обзоре представлены данные по 7 основным отраслям, остальные сферы экономики были объединены в группу «Прочие», так как результаты по ним не являются репрезентативными. На графиках исследования не приведена информация об отраслях из раздела «Прочие», однако результаты учитывались при расчете комплексных (не отраслевых) показателей.

Респонденты



Среднее количество офисов в распределенной системе – 77.
Среднее количество компьютеров в информационной системе (ИС) – 720.

Количество компьютеров в информационной системе



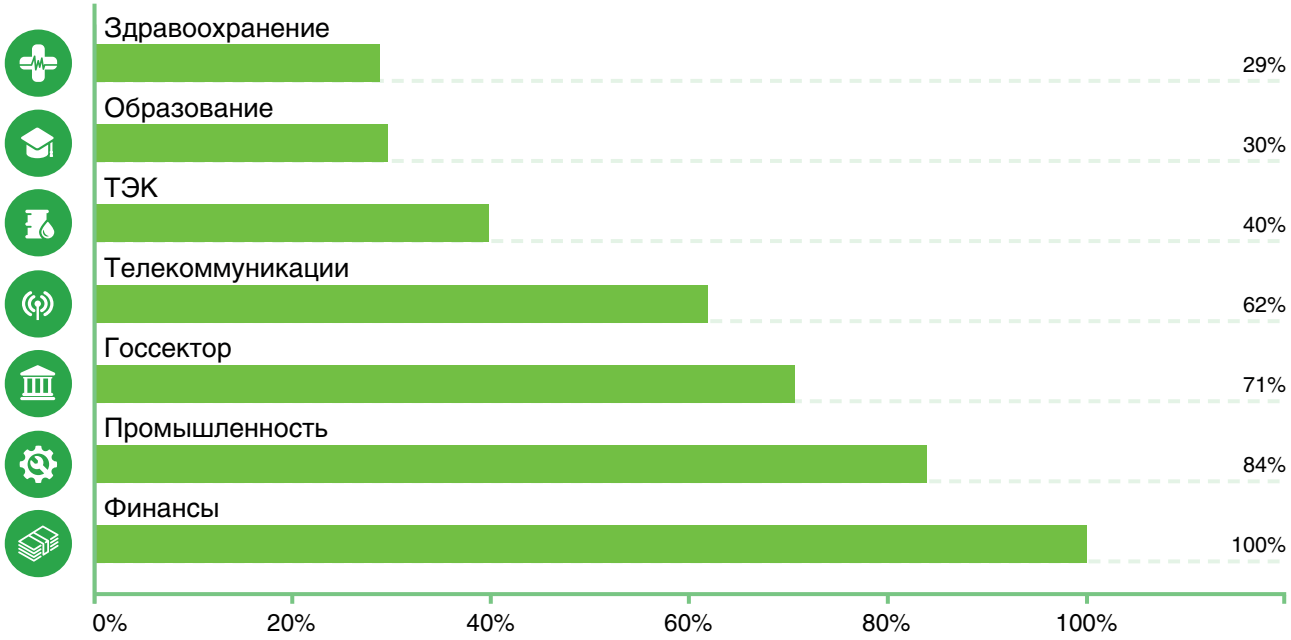
Кто отвечает за информационную безопасность?

В 69% организаций за информационную безопасность отвечает профильный сотрудник. Однако в ряде компаний задачи защиты информации ложатся на сотрудников смежных подразделений, среди них:

- инспектор;
- старший казначей;
- учитель информатики.

Наиболее зрелые отрасли с точки зрения информационной безопасности – финансовая сфера и промышленность. В этих организациях практически всегда вопросами защиты информации занимаются выделенные специалисты. Обратная ситуация – в организациях здравоохранения и образования – здесь обязанности обеспечения ИБ сотрудники чаще всего совмещают с другими задачами.

Профильные специалисты в различных отраслях



Отраслевая специфика:

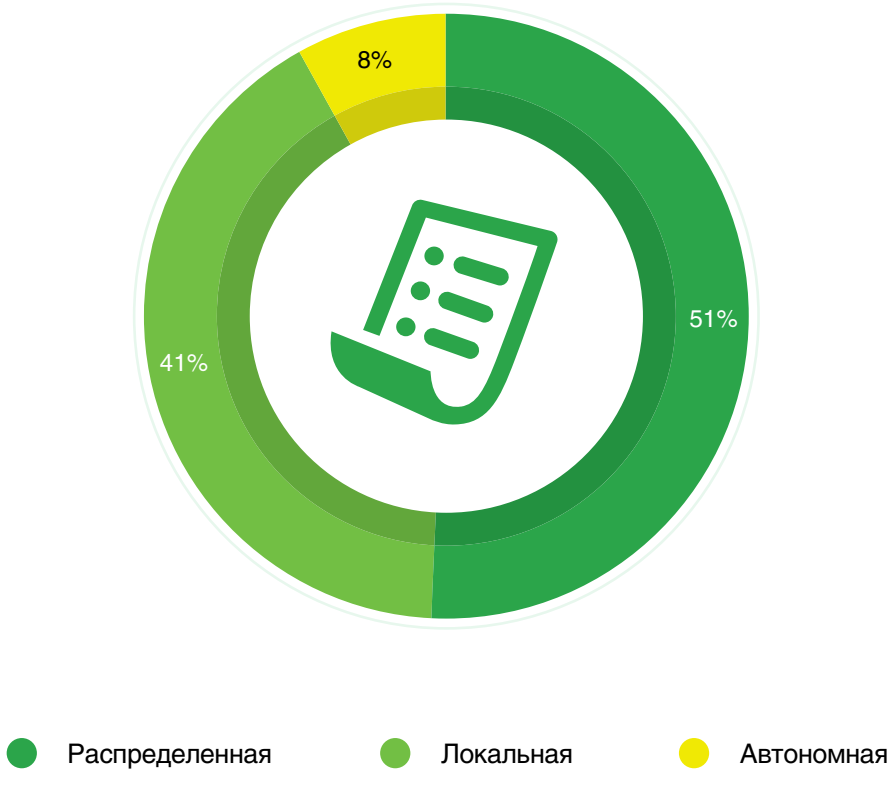
- Для госсектора характерно большое количество наименований должностей, ответственных за ИБ: респонденты назвали 16 вариантов.
- В медицинских учреждениях чаще всего задачи обеспечения информационной безопасности ложатся на штатных программистов, выделенные ИБ-отделы существуют только в 10% организаций.
- В сфере образования должность специалиста по информационной безопасности чаще всего является совмещенной: обязанности выполняют смежные специалисты: программисты, ИТ-инженеры и даже учителя информатики. При этом в 14% образовательных учреждений за защиту информации отвечает начальник ИБ-отдела, что говорит о высоком уровне ИБ-зрелости.

Характеристики информационных систем персональных данных (ИСПДн)

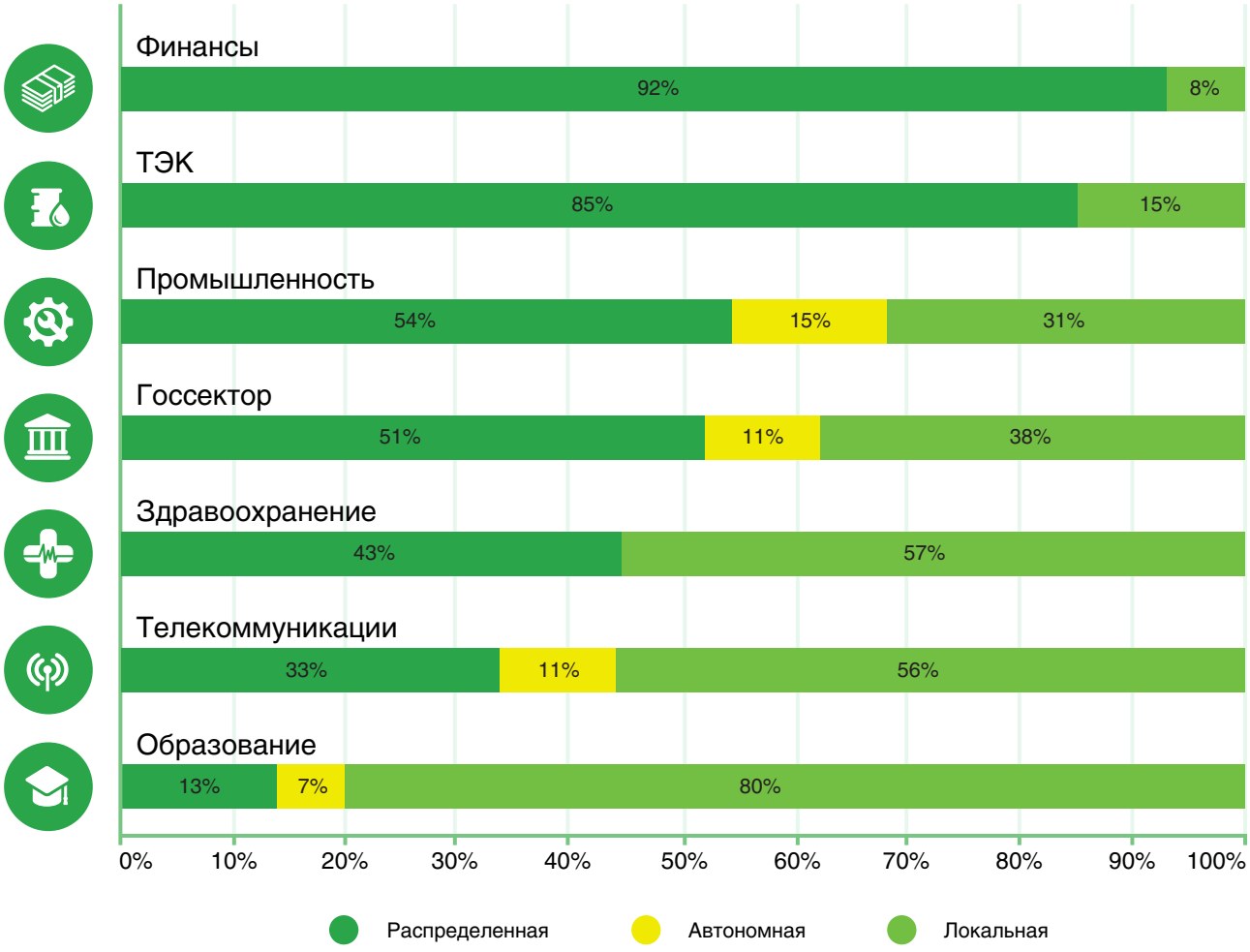
Структура ИСПДн

Существуют три типа информационных систем персональных данных:

- **автономная система** представляет собой не подключенные к иным информационным системам комплексы технических и программных средств, предназначенные для обработки персональных данных;
- **локальная система** – это комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа;
- **распределенная система** включает несколько сетей, размещенных на разных площадках и объединенных в единую систему.



Характеристики информационных систем персональных данных (ИСПДн)

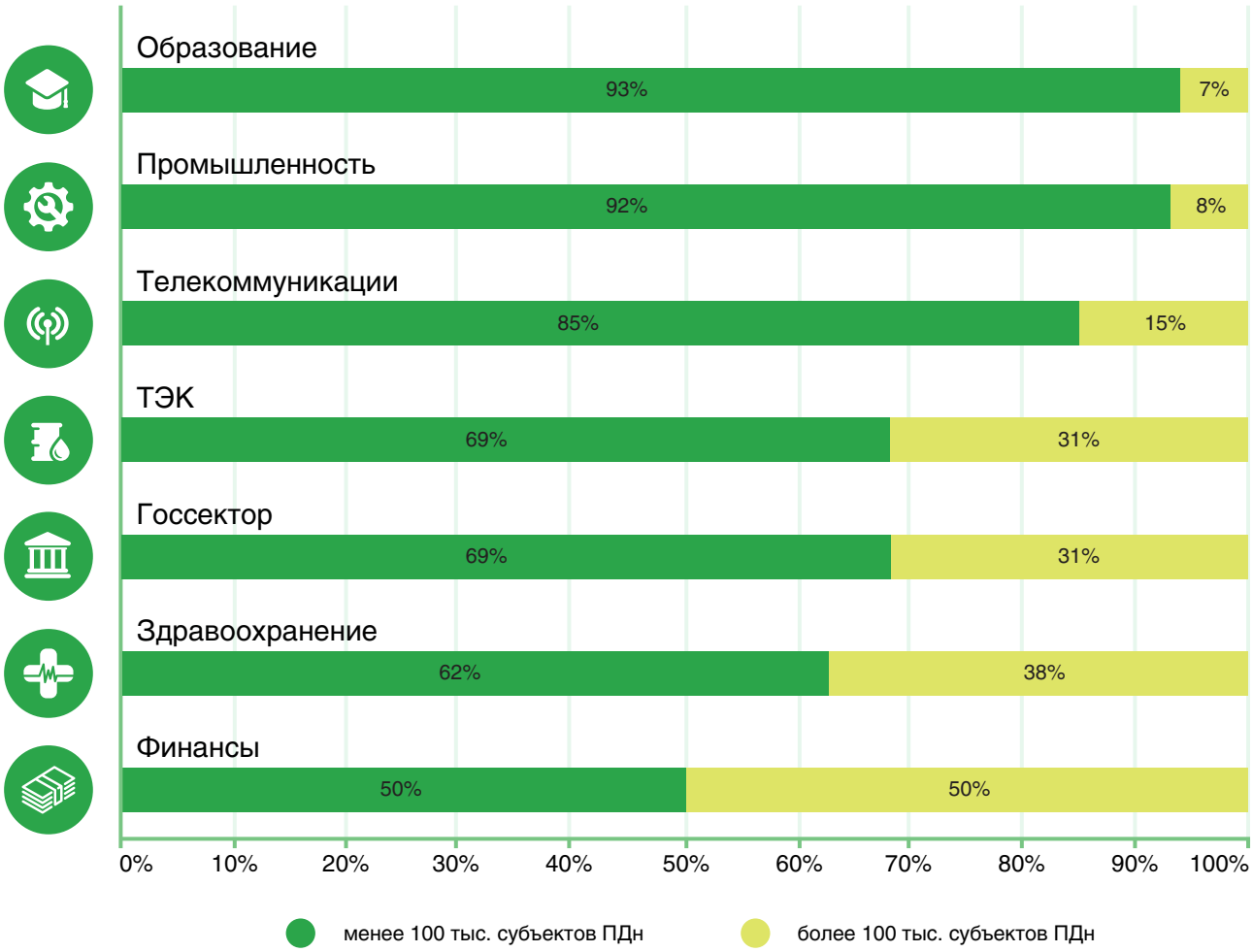


В организациях финансового сектора, нефтегазовых и энергетических компаниях информационные системы практически всегда являются распределенными. Обратная ситуация наблюдается в образовательных учреждениях – здесь они в 87% случаев локальные или автономные.

Характеристики информационных систем персональных данных (ИСПДн)

Объем обрабатываемых персональных данных

¾ организаций обрабатывают персональные данные менее 100 тыс. субъектов.

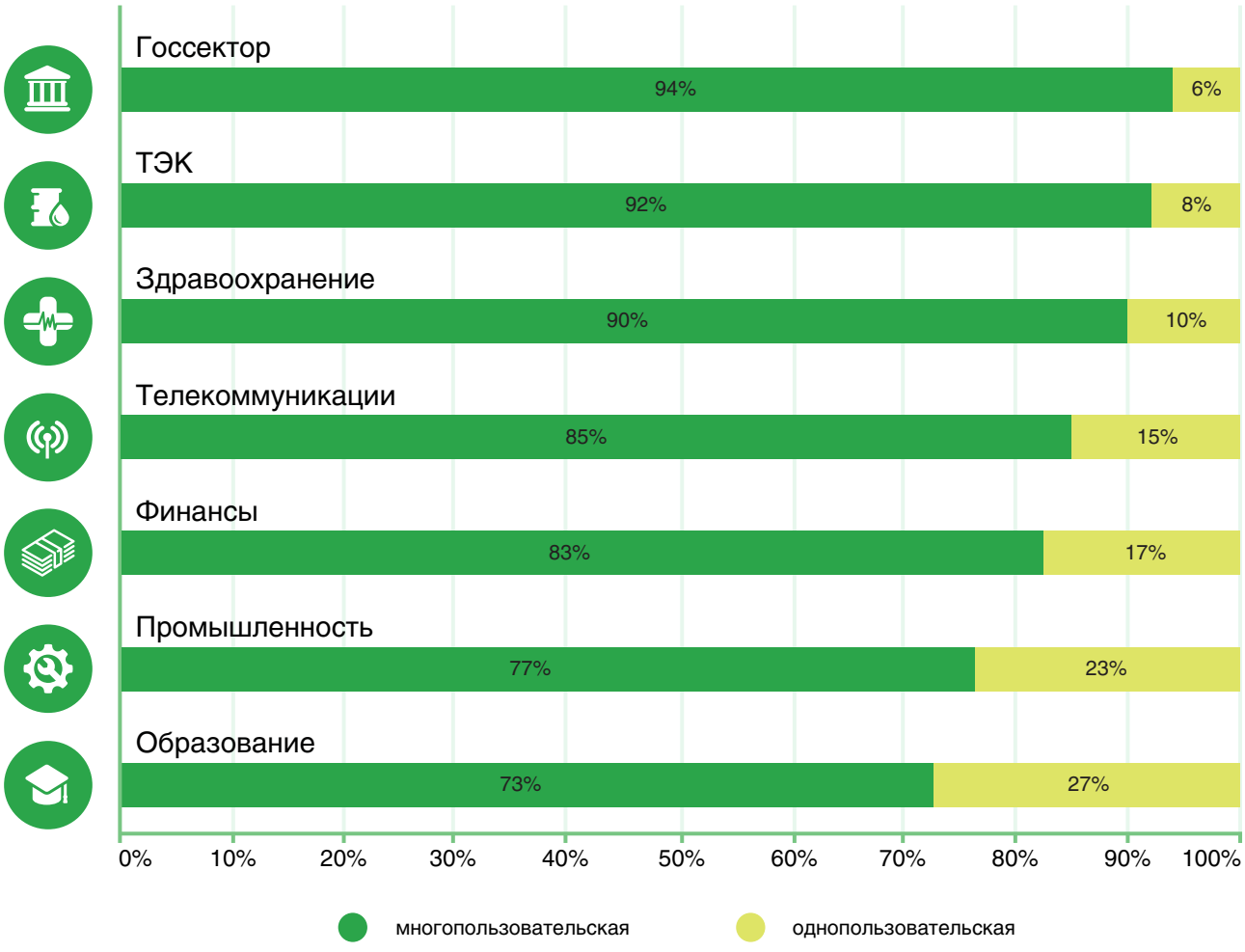


Характеристики информационных систем персональных данных (ИСПДн)

Режим обработки ПДн

Информационная система персональных данных может быть однопользовательской или многопользовательской. В первом случае один сотрудник сочетает в себе роли администратора и пользователя ИСПДн и единолично осуществляет обработку ПДн на одном компьютере. Во всех других случаях ИСПДн является многопользовательской.

Результаты исследования показали, что только 17% ИСПДн являются однопользовательскими, остальные 83% – многопользовательские.

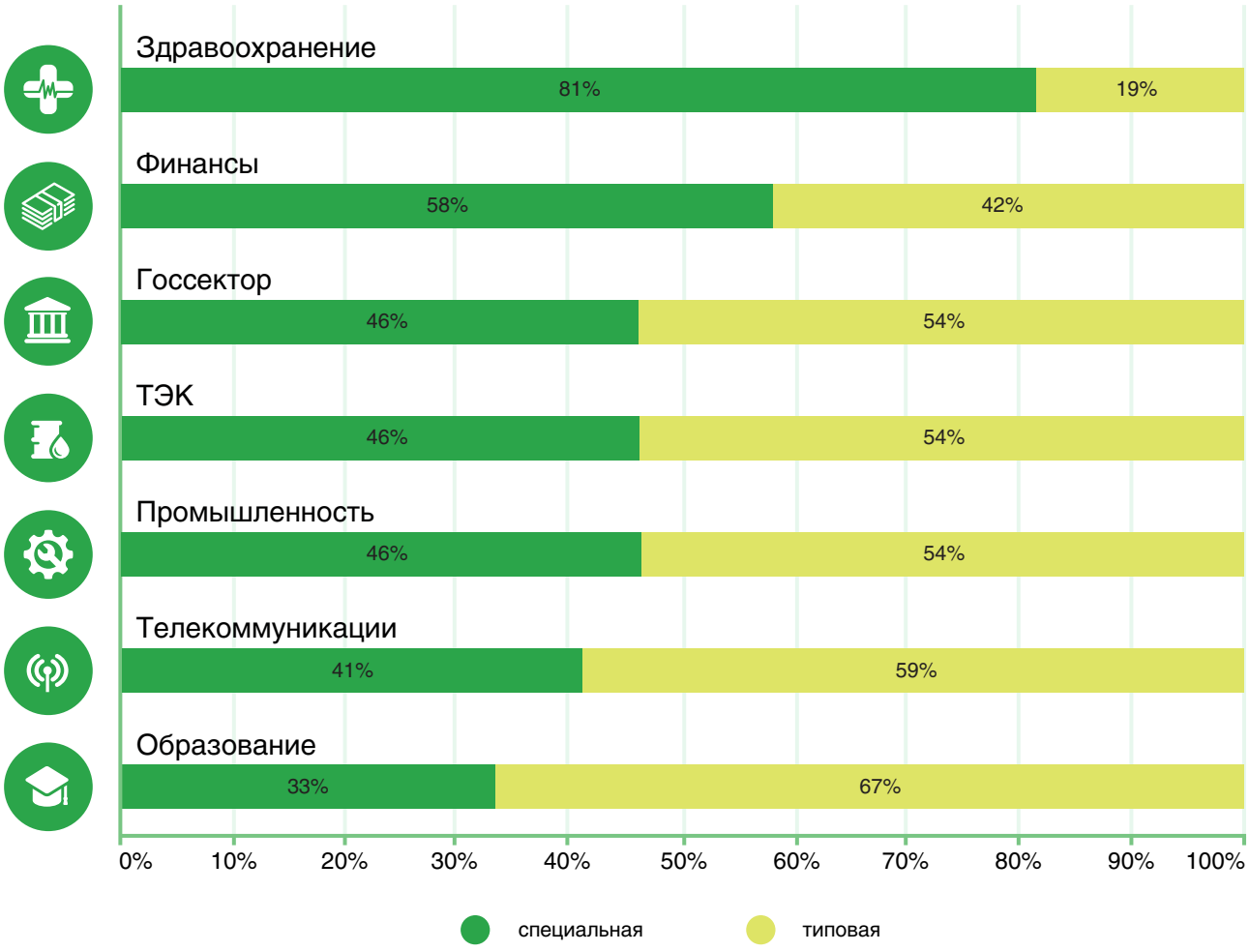


Характеристики информационных систем персональных данных (ИСПДн)

Тип ИСПДн

Типовые ИСПДн – это информационные системы, в которых требуется обеспечить только конфиденциальность ПДн.
Специальные ИСПДн – это информационные системы, в которых кроме конфиденциальности необходимо обеспечить еще хотя бы одну характеристику безопасности персональных данных (целостность, доступность). Кроме того, к специальным системам относятся все ИСПДн, обрабатывающие данные о здоровье субъектов.

В 47% организаций информационная система персональных данных является специальной, в остальных 53% ИСПДн – типовая.
При этом в медицинских организациях более 80% ИСПДн являются специальными (что связано с обработкой данных о здоровье граждан РФ), а в образовании их только 33%.



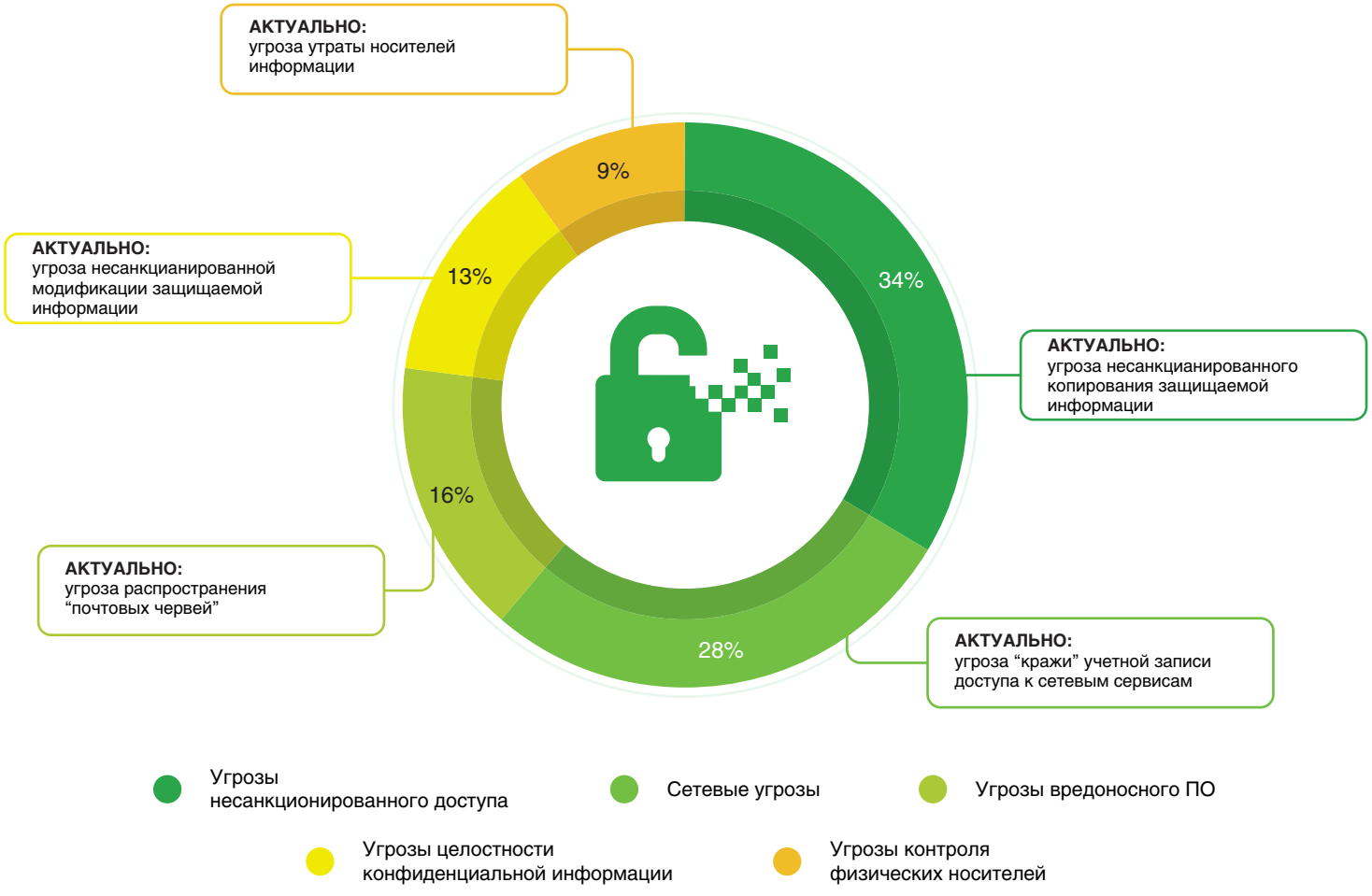
Актуальные угрозы информационной безопасности

Для анализа актуальных угроз безопасности информации на рабочих станциях и серверах были использованы данные, опубликованные на сайте ФСТЭК России. База угроз была поделена на пять основных групп, относящихся к рабочим станциям и серверам:

- угрозы несанкционированного доступа;
- сетевые угрозы;
- угрозы вредоносного ПО;
- угрозы целостности конфиденциальной информации;
- угрозы контроля физических носителей.

В ходе исследования аналитиками «Кода безопасности» были выявлены группы, включающие наибольшее число актуальных угроз, а также определен ТОП-5 угроз информационной безопасности на рабочих станциях и серверах. Кроме того, была произведена оценка наиболее и наименее популярных угроз внутри каждой группы.

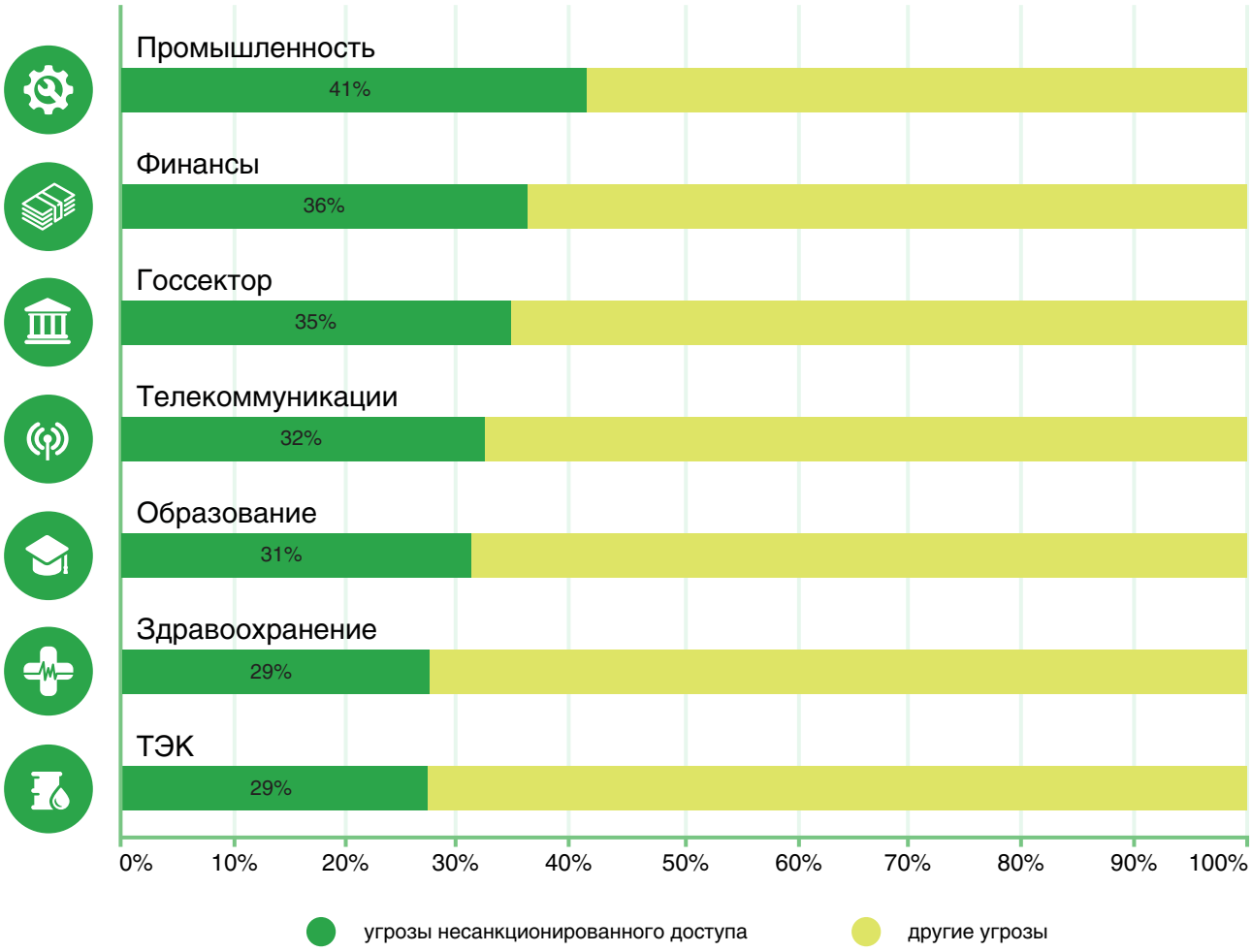
Группы угроз ИБ и ТОП угроз в группах



Актуальные угрозы информационной безопасности

Угрозы несанкционированного доступа

Наибольшую опасность для информации на рабочих станциях и серверах представляют угрозы несанкционированного доступа. Они составили от 29% до 41% от общего числа актуальных угроз безопасности.



Среди угроз несанкционированного доступа стоит особо выделить неправомерное ознакомление с защищаемой информацией и ее несанкционированное копирование. Они оказались актуальны для большинства организаций во всех отраслях *(см. таблицу 1)*.

Данные по наименее актуальным угрозам сильно разнятся: для телеком-компаний и банков это загрузка нештатной операционной системы, а для организаций образовательного и медицинского секторов – угроза несанкционированного создания учетной записи пользователя.

Актуальные угрозы информационной безопасности

Таблица 1. Актуальные угрозы несанкционированного доступа

АКТУАЛЬНЫЕ УГРОЗЫ	Госсектор	Промышленность	ТЭК	Здравоохранение	Образование	Телекоммуникации	Финансы
Угроза доступа к защищаемым файлам с использованием обходного пути	60%	85%	54%	43%	60%	56%	75%
Угроза загрузки нештатной операционной системы	31%	62%	69%	52%	33%	22%	33%
Угроза использования альтернативных путей доступа к ресурсам	48%	69%	62%	52%	60%	52%	67%
Угроза использования механизмов авторизации для повышения привилегий	41%	54%	31%	29%	40%	44%	58%
Угроза обхода некорректно настроенных механизмов аутентификации	41%	46%	54%	29%	47%	48%	50%
Угроза неправомерного ознакомления с защищаемой информацией	68%	85%	100%	62%	67%	74%	83%
Угроза несанкционированного удаления защищаемой информации	72%	69%	46%	48%	67%	59%	75%

Актуальные угрозы информационной безопасности

АКТУАЛЬНЫЕ УГРОЗЫ	Госсектор	Промышленность	ТЭК	Здравоохранение	Образование	Телекоммуникации	Финансы
Угроза несанкционированного восстановления удаленной защищаемой информации	35%	46%	31%	14%	40%	33%	33%
Угроза несанкционированного доступа к аутентификационной информации	48%	62%	23%	38%	47%	52%	58%
Угроза несанкционированного изменения аутентификационной информации	35%	46%	38%	19%	47%	44%	50%
Угроза несанкционированного создания учетной записи пользователя	36%	46%	46%	10%	27%	37%	42%
Угроза несанкционированного копирования защищаемой информации	74%	92%	46%	57%	47%	74%	83%
Угроза несанкционированного управления буфером	25%	31%	31%	19%	33%	41%	42%

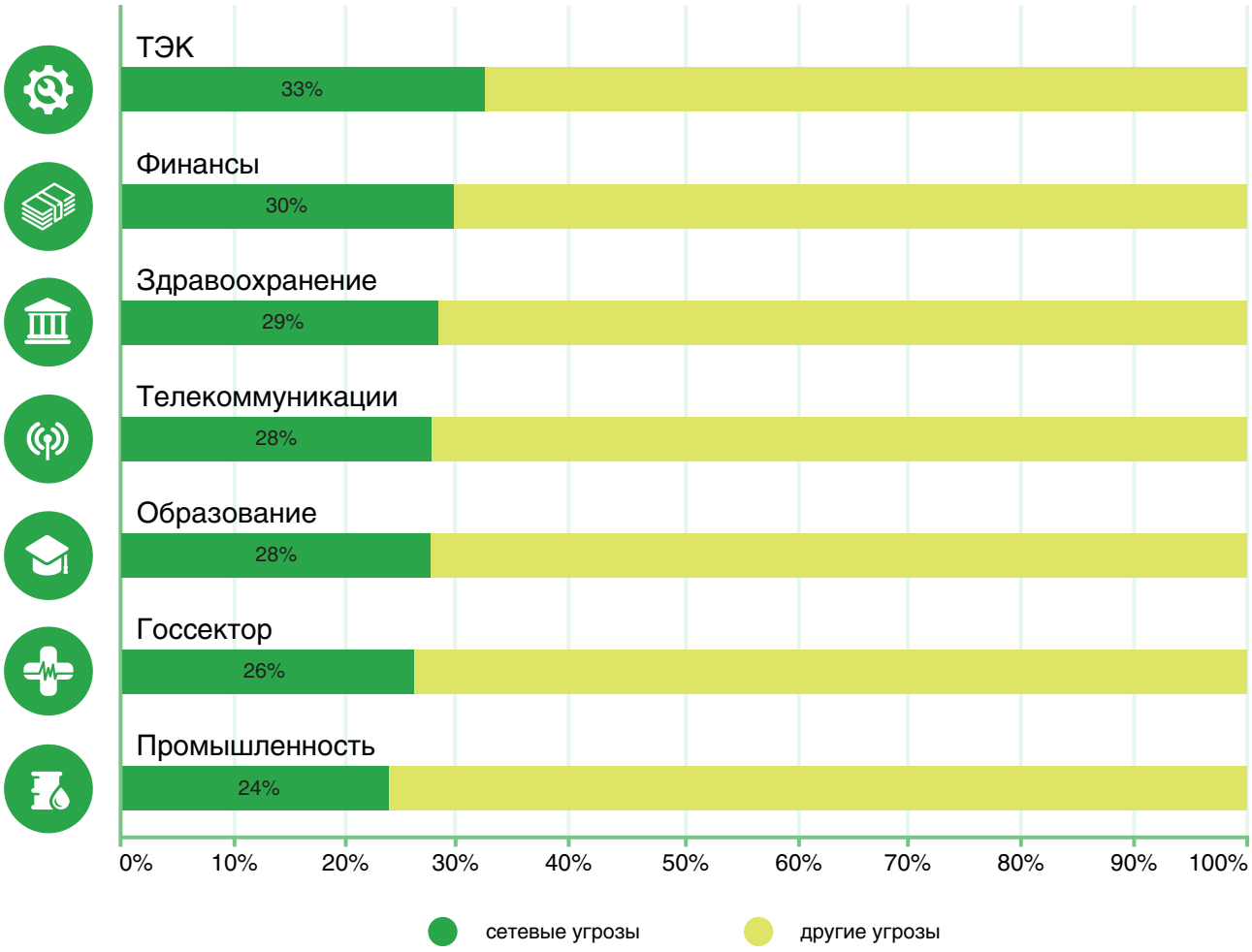
наиболее актуальная угроза

наименее актуальная угроза

Актуальные угрозы информационной безопасности

Сетевые угрозы

Сетевые угрозы занимают вторую позицию, составляя около 28% от общего числа актуальных угроз безопасности.



Наиболее актуальной угрозой почти для всех отраслей стала «кража» учетной записи доступа к сетевым ресурсам. Представители финансового сектора особо выделили угрозу проведения атак типа «отказ в обслуживании» (DOS). Из менее актуальных угроз в данной группе можно выделить определение типов объектов защиты и получение предварительной информации об объекте защиты. Следовательно, сегодня мало кто всерьез задумывается о необходимости защиты от кибер разведки, что в конечном итоге повышает вероятность успешного взлома систем злоумышленником.

Актуальные угрозы информационной безопасности

Таблица 2. Актуальные сетевые угрозы

АКТУАЛЬНЫЕ УГРОЗЫ	Госсектор	Промышленность	ТЭК	Здравоохранение	Образование	Телекоммуникации	Финансы
Угроза неправомерных действий в каналах связи	53%	54%	54%	57%	47%	52%	50%
Угроза определения топологии вычислительной сети	22%	31%	31%	19%	27%	30%	42%
Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	53%	54%	46%	57%	53%	48%	50%
Угроза обнаружения хостов	26%	31%	38%	29%	27%	37%	42%
Угроза определения типов объектов защиты	30%	23%	15%	24%	20%	41%	50%
Угроза передачи данных по скрытым каналам	37%	23%	54%	43%	53%	41%	33%
Угроза перехвата данных, передаваемых по вычислительной сети	44%	38%	62%	38%	67%	52%	75%

Актуальные угрозы информационной безопасности

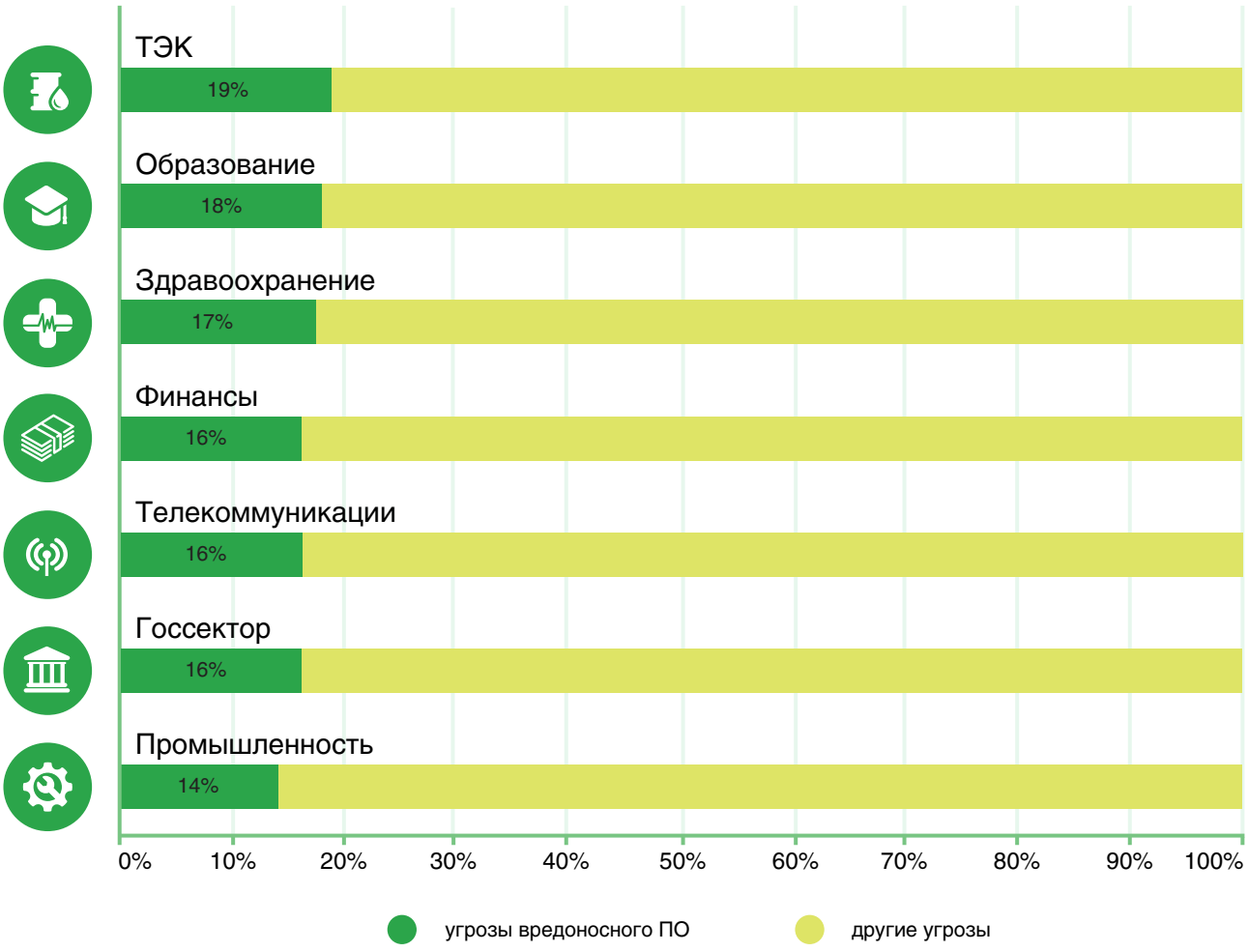
АКТУАЛЬНЫЕ УГРОЗЫ	Госсектор	Промышленность	ТЭК	Здравоохранение	Образование	Телекоммуникации	Финансы
Угроза подмены содержимого сетевых ресурсов	23%	31%	38%	33%	53%	33%	33%
Угроза подмены субъекта сетевого доступа	27%	23%	54%	24%	47%	37%	33%
Угроза получения предварительной информации об объекте защиты	26%	23%	23%	19%	20%	19%	42%
Угроза приведения системы в состояние "отказ в обслуживании" (DOS)	40%	46%	54%	38%	53%	52%	83%
Угроза пропуска проверки целостности программного обеспечения	28%	23%	15%	24%	33%	41%	42%
Угроза "кражи" учетной записи доступа к сетевым сервисам	48%	69%	69%	62%	60%	63%	50%

наиболее актуальная угроза

наименее актуальная угроза

Актуальные угрозы информационной безопасности

Угрозы вредоносного программного обеспечения



Наименее актуальной среди угроз вредоносного программного обеспечения (ПО) большинством специалистов была признана угроза некорректного использования функционала ПО, а вот угроза распространения «почтовых червей» была признана самой опасной.
Угрозу внедрения кода или данных, к которой относится и заражение компьютеров вирусами-шифровальщиками, также выделили многие компании. Особое внимание этой проблеме уделяют организации финансового сектора. Однако, несмотря на опасность и сложность восстановления данных, угроза с точки зрения ИБ-специалистов все-таки уступила по опасности «почтовым червям».

Актуальные угрозы информационной безопасности

Таблица 3. Актуальные угрозы вредоносного ПО

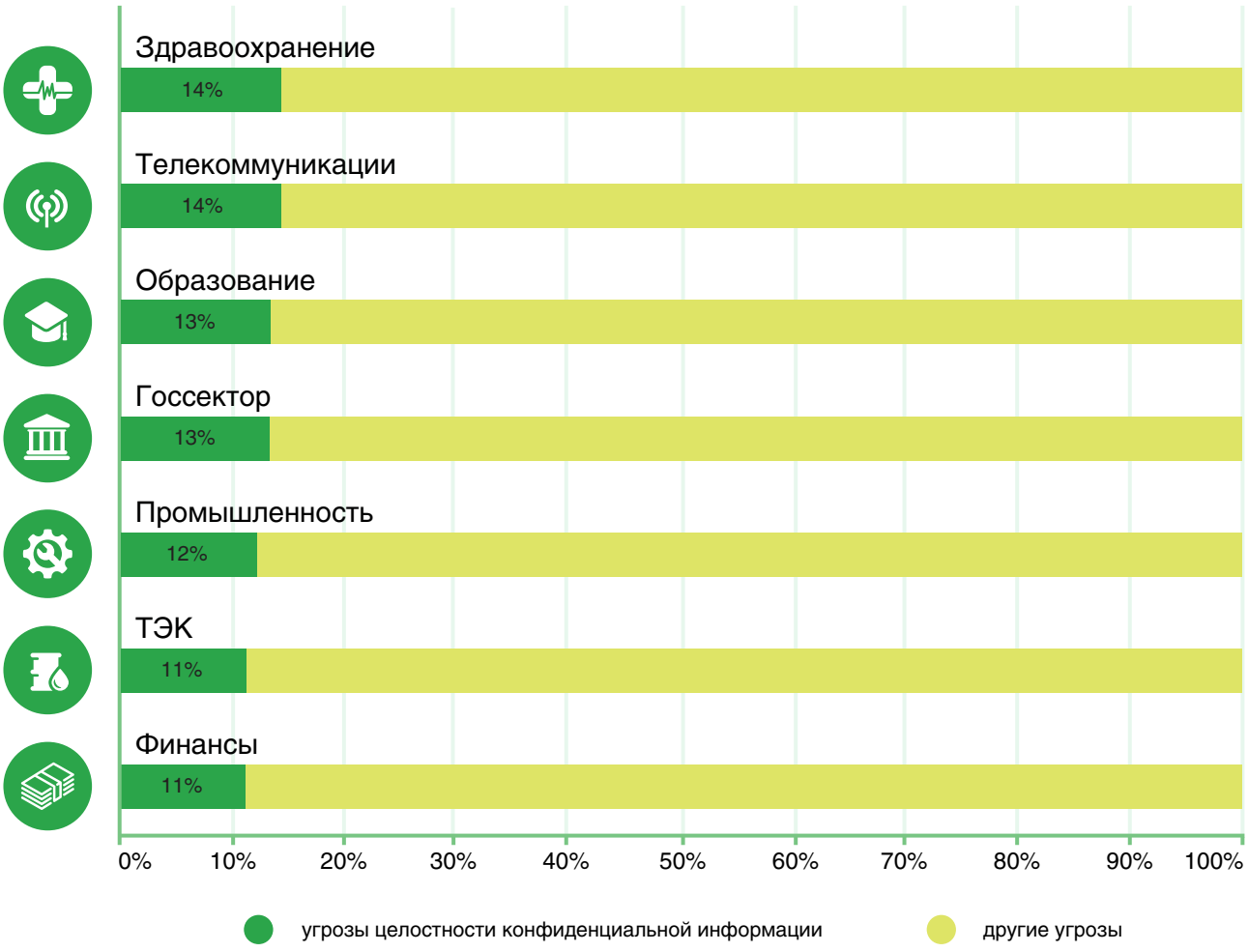
АКТУАЛЬНЫЕ УГРОЗЫ	Госсектор	Промышленность	ТЭК	Здравоохранение	Образование	Телекоммуникации	Финансы
Угроза внедрения кода или данных	58%	77%	62%	67%	73%	52%	92%
Угроза некорректного использования функционала программного обеспечения	54%	54%	46%	29%	47%	52%	33%
Угроза заражения компьютера при посещении неблагонадежных сайтов	53%	62%	69%	62%	87%	78%	50%
Угроза неправомерного шифрования информации	58%	31%	69%	62%	53%	52%	75%
Угроза распространения "почтовых червей"	60%	46%	85%	62%	87%	78%	75%

наиболее актуальная угроза

наименее актуальная угроза

Актуальные угрозы информационной безопасности

Угрозы целостности конфиденциальной информации



Распределение угроз целостности конфиденциальной информации по отраслям оказалось практически равномерным: самой опасной считается реализация угрозы несанкционированной модификации защищаемой информации, а наименее опасной – угроза несанкционированного редактирования реестра.

Актуальные угрозы информационной безопасности

Таблица 4. Актуальные угрозы целостности конфиденциальной информации

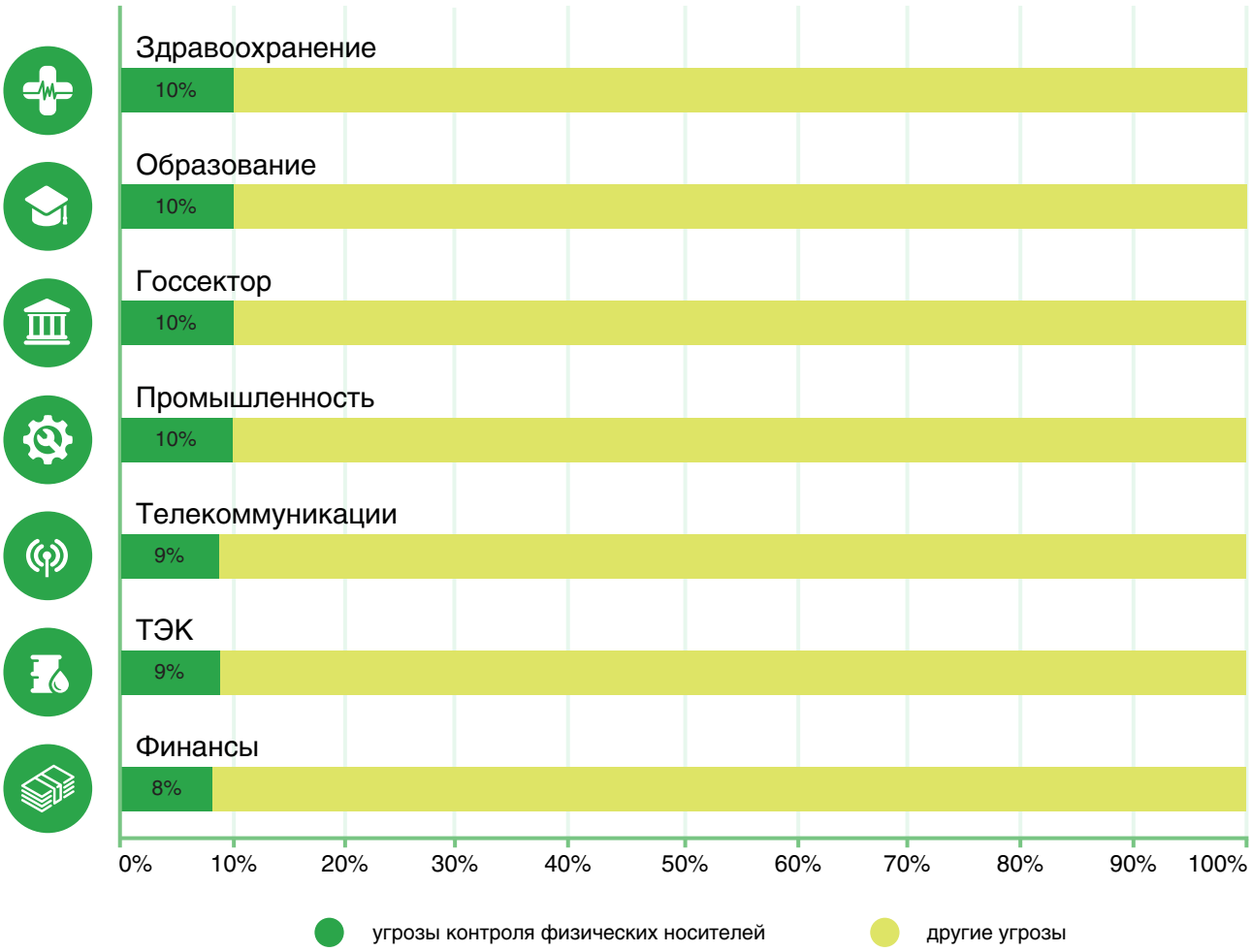
АКТУАЛЬНЫЕ УГРОЗЫ	Госсектор	Промышленность	ТЭК	Здравоохранение	Образование	Телекоммуникации	Финансы
Угроза деструктивного изменения конфигурации/ среды окружения программ	47%	62%	54%	52%	47%	78%	58%
Угроза несанкционированного редактирования реестра	43%	38%	31%	48%	53%	56%	33%
Угроза повреждения системного реестра	53%	46%	31%	52%	87%	63%	42%
Угроза несанкционированной модификации защищаемой информации	73%	77%	69%	76%	67%	81%	83%

наиболее актуальная угроза

наименее актуальная угроза

Актуальные угрозы информационной безопасности

Угрозы контроля физических носителей



Актуальность угроз контроля физических носителей совпадает для всех отраслей: наибольший риск представляет утрата носителей информации с сохраненными на них конфиденциальными данными. Меньший риск представляют угрозы изменения компонентов системы.

Актуальные угрозы информационной безопасности

Таблица 5. Актуальные угрозы контроля физических носителей

АКТУАЛЬНЫЕ УГРОЗЫ	Госсектор	Промышленность	ТЭК	Здравоохранение	Образование	Телекоммуникации	Финансы
Угроза изменения компонентов системы	44%	38%	31%	43%	40%	30%	42%
Угроза утраты носителей информации	68%	85%	69%	62%	87%	78%	58%
Угроза хищения средств хранения, обработки и (или) ввода/вывода/ передачи информации	57%	62%	54%	52%	53%	63%	50%

наиболее актуальная угроза

наименее актуальная угроза

Актуальные угрозы информационной безопасности

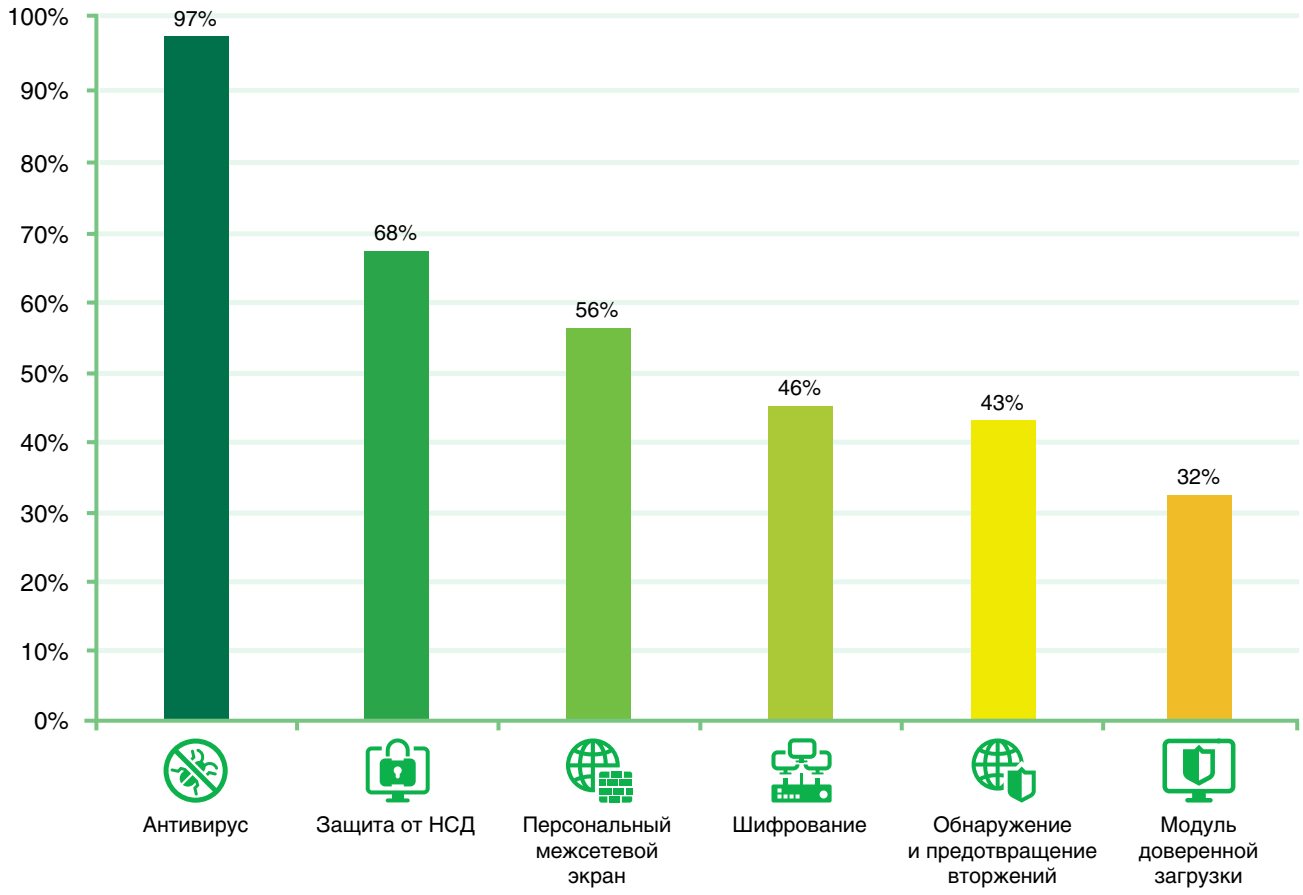
ТОП-5 угроз безопасности

Таким образом, ТОП-5 угроз безопасности информации на рабочих станциях и серверах выглядит следующим образом:

Средства защиты рабочих станций и серверов

Результаты исследования свидетельствуют о том, что на защиту рабочих станций, серверов и сетевого взаимодействия каждая компания тратит в среднем 53% ИБ-бюджета.

Популярные средства защиты рабочих станций и серверов



Антивирус установлен на компьютерах 97% участников опроса. Использование антивируса для защиты рабочих станций и серверов – формат обеспечения безопасности по умолчанию. Средство защиты от НСД установлено в 68% организаций, в большей степени они востребованы в госсекторе и финансовой сфере.

Более половины участников исследования используют персональный межсетевой экран.

Только 1/3 организаций используют модуль доверенной загрузки (МДЗ). При этом не удается выделить какую-либо отрасль, где эти средства применялись бы чаще других: они в равной степени интересны предприятиям госсектора, нефтегазовой и энергетической отраслей, сферы образования и финансового сектора.

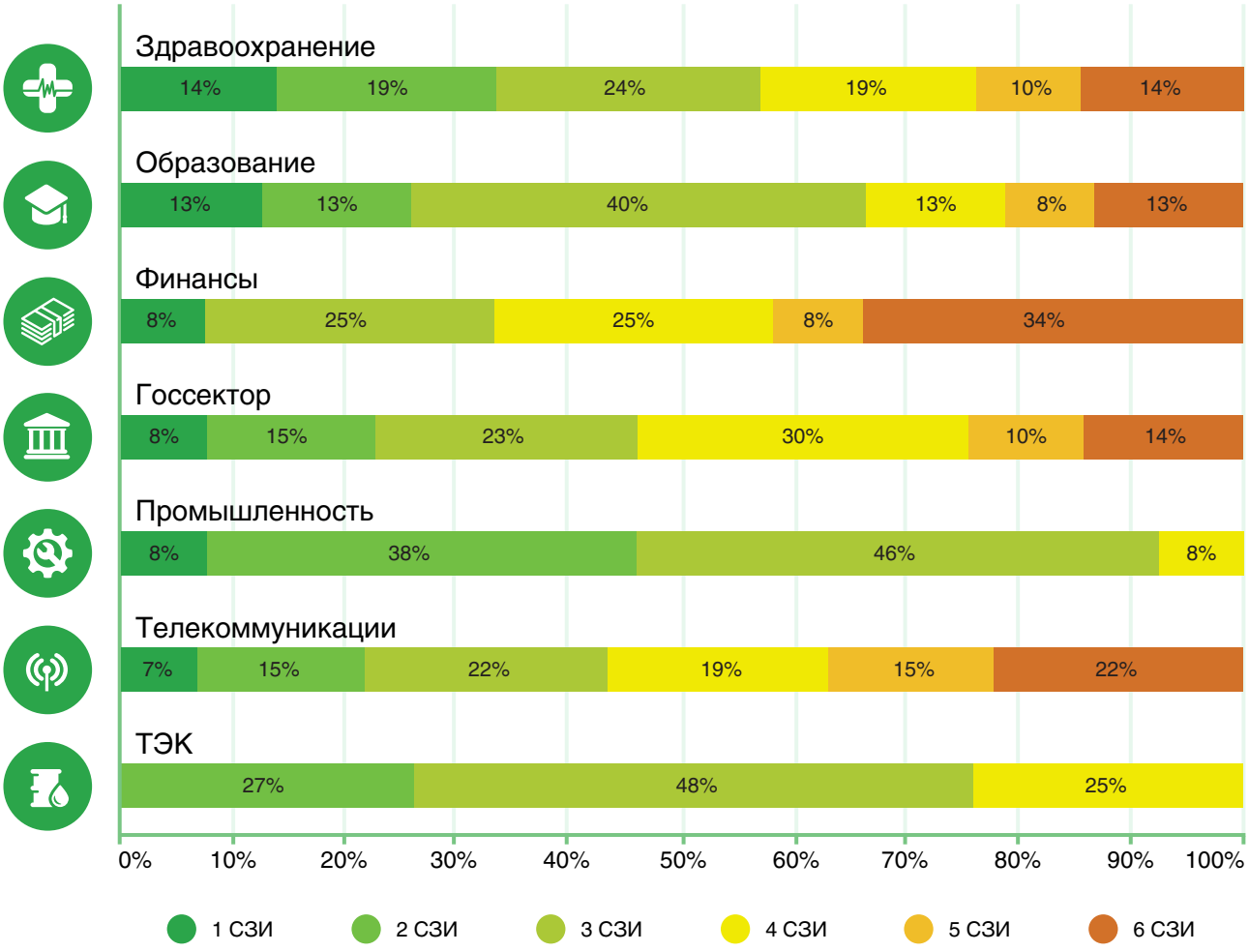
Отметим, что при среднем показателе применения средств шифрования в 46% организации промышленного сектора используют такой метод защиты значительно реже: только 15% компаний применяют для защиты данных СКЗИ.

Средства защиты рабочих станций и серверов

Количество средств защиты на одном компьютере

Среднее число средств защиты, одновременно работающих на одном компьютере, – 3. Эти данные сильно разнятся по отраслям. Например, финансовые компании для защиты рабочих станций и серверов в большинстве случаев (34%) используют сразу 6 средств защиты. С ними солидарны и телекоммуникационные компании – в 22% случаев они применяют 6 средств защиты. В госсекторе каждая третья компания применяет 4 СЗИ, а в здравоохранении, образовании, промышленности, топливно энергетическом комплексе показатели равны средним – 3 средства защиты на одном компьютере.

На сегодняшний день всего 8% организаций используют для защиты информации лишь одно средство. Это говорит о дефиците комплексных решений, которые позволили бы реализовать все задачи обеспечения безопасности данных на компьютерах.



Заключение

В ходе исследования аналитиками «Кода безопасности» были опрошены более 500 респондентов из различных отраслей российской экономики. Результаты показали, что большая часть информационных систем в организациях является распределенной (в среднем 77 офисов) и включает в себя 720 компьютеров.

ОСНОВНЫЕ РИСКИ

Респонденты обозначили актуальные угрозы безопасности информации, которая обрабатывается и/или хранится на рабочих станциях и серверах. Среди выделенных 5 групп рисков наибольшее внимание уделяется угрозам несанкционированного доступа (их отметили в 34% случаев) и сетевым угрозам (28%).

БОЛЬШОЙ ПАРК СРЕДСТВ ЗАЩИТЫ

Чтобы защитить компьютеры, организации используют в среднем 3 наложенных средства защиты. Показатель этот различается в зависимости от отрасли: в финансовых и телеком- муникационных компаниях часто применяют 6 СЗИ, в госсекторе – 4 средства защиты на одной рабочей станции.

МАЛО ПРОФИЛЬНЫХ СПЕЦИАЛИСТОВ

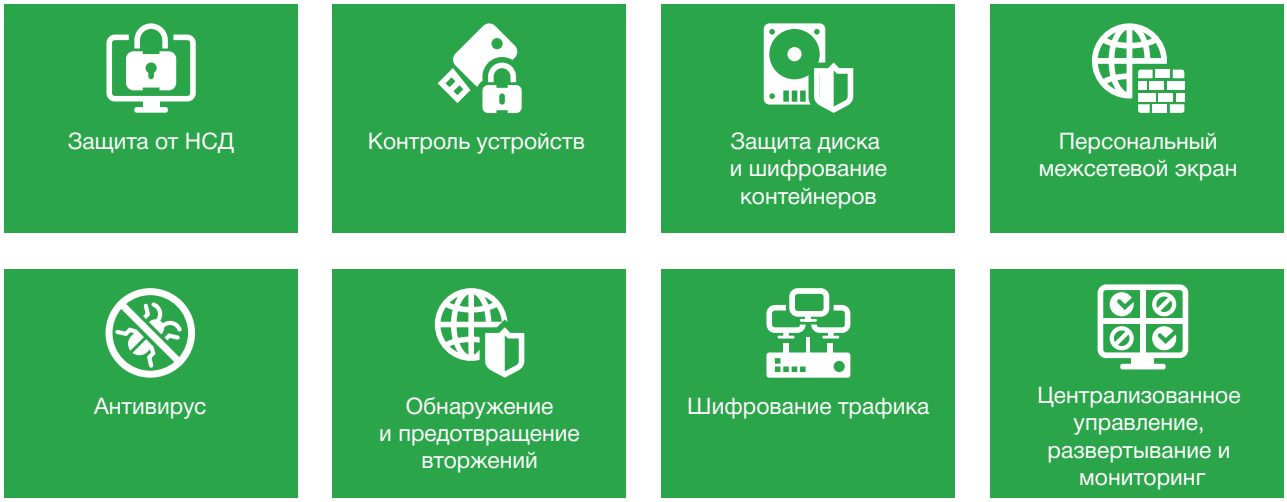
Несмотря на масштаб информационных систем и необходимость обеспечивать поддержку целого набора СЗИ, во многих организациях (31%) до сих пор безопасность на местах обеспечивают непрофильные специалисты. Это означает, что справиться с техническими проблемами взаимодействия средств защиты, администрирования СЗИ и расследования инци- дентов локально практически невозможно.

Основная задача по управлению системой ложится на центральный офис, специалисты которого часто не видят проблем в региональных структурах и не могут определить причину неполадки, даже общаясь с технической поддержкой всех разработчиков средств защиты. В результате, несмотря на большое количество установленных на компьютере СЗИ, компании не всегда могут обеспечить требуемый им уровень информационной безопасности: злоумышленникам проще найти уязвимость в нестабильной системе, сконфигурированной из различных защитных продуктов.

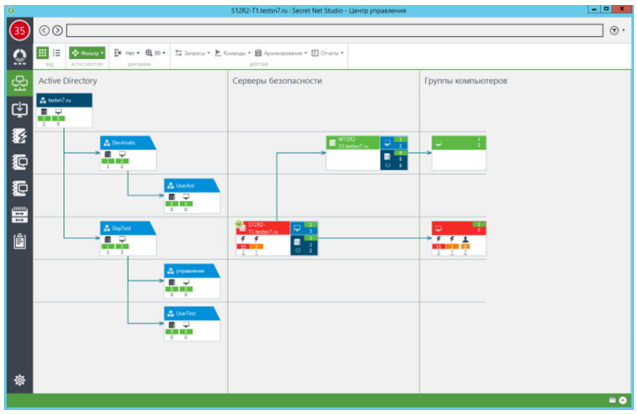
Заключение

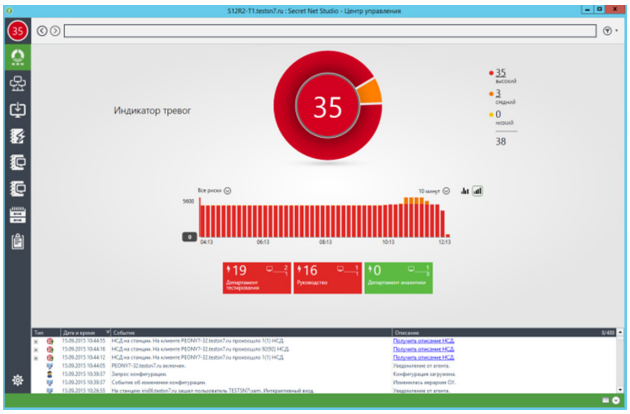
SECRET NET STUDIO

Решением такой проблемы может стать применение комплексного средства защиты рабочих станций и серверов. СЗИ Secret Net Studio разработки компании «Код безопасности» обеспечивает защиту компьютеров на 5 уровнях (данных, приложений, сети, операционной системы и периферийного оборудования) и объединяет под общим управлением более 20 защитных механизмов.



Применение Secret Net Studio позволяет полностью перевести функции администрирования системы в центральный офис, установив на клиентских устройствах общие политики безопасности. Никаких действий администраторам на местах производить не нужно, что позволяет снять с непрофильных специалистов ответственность за техническую поддержку средств защиты информации. Любые инциденты отображаются на общей панели мониторинга, где также осуществляется корреляция данных о событиях безопасности для получения комплексной картины о состоянии защищенности рабочих станций и серверов. Вопросы технической поддержки продукта решаются в режиме «единого окна» вместе со специалистами компании «Код безопасности».





Больше о Secret Net Studio на сайте компании «Код Безопасности»

Код Безопасности

«Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, облачных сред, мобильных устройств, а также коммерческой и государственной тайны. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

Тел.: +7 (495) 982 30 20

buy@securitycode.ru

www.securitycode.ru