

ОКБ САПР: ОТРАЖАЕМ КИБЕРАТАКИ

www.okbsapr.ru,
okbsapr@okbsapr.ru



СОДЕРЖАНИЕ

1	Введение.....	3
2	Причины роста числа кибератак	5
	2.1 Удалённая работа сотрудников	6
	2.2 Бесконтрольные действия пользователей	8
	2.3 Развитие инструментария злоумышленников	10
	2.4 Делегирование задач подрядным организациям (аутсорсинг)	11
	2.5 Кибератаки и способы их отражения	12
3	Защита от кибератак	14
4	Решения для защиты информационных ресурсов.....	16
	4.1 Средства защиты удалённого доступа	18
	4.1.1 СОДС «МАРШ!» и «М!&М»	19
	4.1.2 «TrusT Удалёнка».....	22
	4.1.3 Двухконтурный моноблок.....	25
	4.1.4 Защищённые терминалы «m-TrusT Терминал» и «Центр-TrusT»	26
	4.1.5 Криптошлюзы fin-TrusT.....	29
	4.1.6 Trust-in-Motion	32
	4.2 Средства контроля точек подключения сторонних организаций	36
	4.2.1 МЭ-TrusT.....	37
	4.3 Средства контроля информационной инфраструктуры	38
	4.3.1 Средства защиты от вредоносного инструментария	41
	4.3.2 Средства контроля за работой пользователей	70
	4.3.3 Специальные инструменты для управления встроенными механизмами безопасности	93
5	Отражаем кибератаки.....	97

1 ВВЕДЕНИЕ

Кибератака. В последнее время это слово можно слышать отовсюду – атакованы могут быть банки, больницы, школы, социальные сети, промышленные структуры, госсектор и другие отрасли.

Кибератаку можно трактовать как совокупность противоправных действий, совершаемых злоумышленниками по отношению к информационной системе, с целью завладеть информацией или денежными средствами, нарушить целостность структуры информационной системы или ее программ и данных, перехватить управление инфраструктурой системы.

Как правило, основными целями кибератак являются перехват управления инфраструктурой, кража денежных средств или информации ограниченного доступа, вывод из строя элементов инфраструктуры, подмена сетевого трафика и т.д.

С каждым годом число кибератак неизменно растёт. По данным¹⁾ компании Solar JSOC, за прошедший год возросло число целевых атак, из числа которых популярными стали атаки на перехват управления. Также в рамках отчета Solar JSOC выделены в отдельную категорию атаки типа Supply Chain¹⁾ (атака через подрядчика). За прошедший год количество таких атак на объекты критических информационных инфраструктур (КИИ) увеличилось в два раза.

Среди инструментов нарушителей лидируют²⁾:

- применение вредоносного программного обеспечения (ВрПО), в особенности, фишинга и программ-шифровальщиков;
- поиск уязвимостей в приложениях;
- Brute force¹⁾ и компрометация учетных данных внешних сервисов клиента;
- ddos-атаки.

В презентации, опубликованной на портале TAdviser³⁾, компания Solar JSOC выделяет три основных способа совершения атак:

- взлом веб-приложений (поиск уязвимостей приложений);
- социальная инженерия;
- взлом инфраструктуры подрядчиков организации.

Кибератаки тесно связаны с развитием компьютерной техники и прикладных приложений.

Сегодня вычислительные технологии развиваются семимильными шагами еще и под эгидой идеи оптимизации (одно устройство должно выполнять массу действий, быть универсальным). С одной стороны, техника становится мощнее, интеллектуальнее и мобильнее: объем памяти увеличивается, круг программ-приложений расширяется,

¹⁾ Ежегодный отчет Solar JSOC Security Report (<https://rt-solar.ru/analytics/reports/2135/>).

²⁾ Отчет Solar JSOC Security Report. Итоги года (https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf).

³⁾ Кибератаки. Интернет-портал TAdviser (https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8#.D0.98.D0.BD.D1.81.D1.82.D1.80.D1.83.D0.BC.D0.B5.D0.BD.D1.82.D1.8B_.D0.B0.D1.82.D0.B0.D0.BA).

размеры корпусов уменьшаются – и это хорошо. На сегодняшний день практически любой деятельностью можно заниматься, не выходя из дома, в том числе, и профессиональной. Идея оптимизации производства привела также к популярности передачи части профессиональных обязанностей организации-подрядчику в случае, если в этом есть выгода для организации-заказчика.

Однако, с другой стороны, развитие техники и рост числа прикладных программ играет не только положительную роль. Совершенствование вычислительных технологий, универсализация техники, «штамповка» приложений в короткие сроки, что называется «на коленке», приводят к возникновению уязвимостей. Любая уязвимость – это открытая дверь в систему для хакеров. Рост числа уязвимостей и отсутствие наказания за совершённые противоправные поступки, приводят, в свою очередь, к увеличению числа хакеров, инструментарий которых также совершенствуется, вместе с остальными информационными технологиями.

Все это прямо или косвенно приводит к росту числа кибератак.

2 ПРИЧИНЫ РОСТА ЧИСЛА КИБЕРАТАК

Явления, широкое распространение которых привело к увеличению числа атак на информационные системы, можно сгруппировать следующим образом:

- удалённая работа сотрудников;
- бесконтрольные действия пользователей;
- развитие инструментария злоумышленников;
- делегирование выполнения какой-либо деятельности подрядным организациям (аутсорсинг).

Популярные типы кибератак¹⁾, распространённые способы их проведения, а также часто используемый инструментарий показаны на рисунке 1.

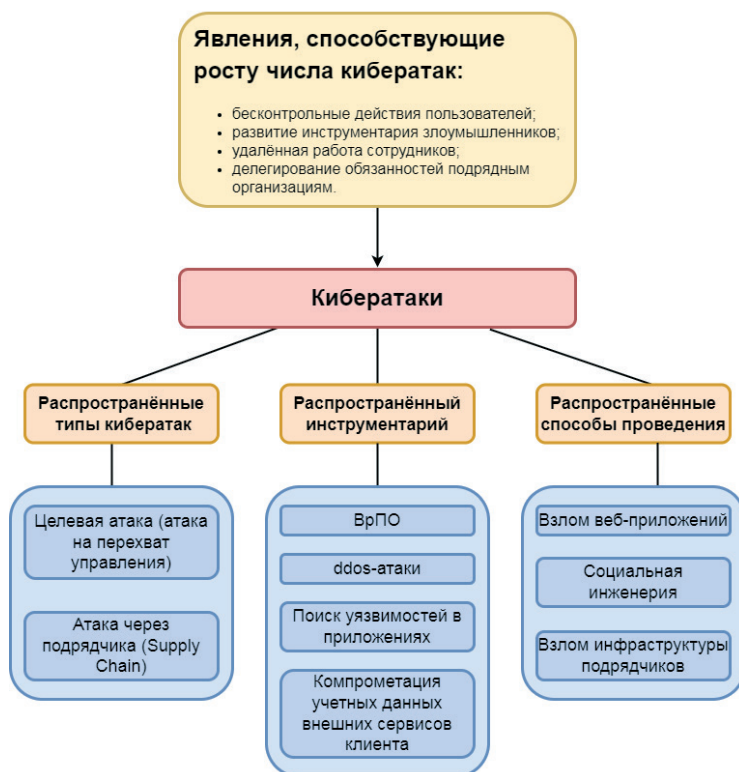


Рисунок 1 - Кибератаки. Распространенные типы, инструментарий, способы проведения

¹⁾ Отчет Solar JSOC Security Report. Итоги года (https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf).

Далее рассмотрим детально, почему эти явления получили массовое распространение в современном обществе, к чему они могут привести, какие есть способы защиты от атак, связанных с каждой из групп явлений, а также какие средства можно использовать для реализации этих способов.

2.1 УДАЛЁННАЯ РАБОТА СОТРУДНИКОВ

Сегодня многие сотрудники работают удалённо, находясь за пределами организации. Одним из поводов массового перехода на «удалёнку» стала начавшаяся в 2020 году пандемия.

Сейчас можно с уверенностью сказать, что многие компании оказались неготовыми к удалённой работе. Некоторые из них до конца не понимали, какие именно решения необходимы для организации безопасного удалённого доступа сотрудников.

Ускоренный переход на «удалёнку» в условиях недостаточности знаний в этой сфере, а также послабление контроля за выходом сотрудников за контролируемую зону привели к возникновению большого числа «белых пятен» в структуре подсистемы информационной безопасности компаний, а вследствие этого, к утечке и компрометации корпоративных данных.

Работа пользователей «из дома» не осталась без внимания злоумышленников. Участились удары хакеров по домашним сетям пользователей – заметное количество атак было направлено именно на них, и неспроста – через личные компьютеры и другие персональные устройства сотрудников легко получить доступ к корпоративным сетям, устройствам и данным, так как, зачастую, сеть, которой пользуется сотрудник, находясь дома, защищена заметно слабее, чем корпоративная.

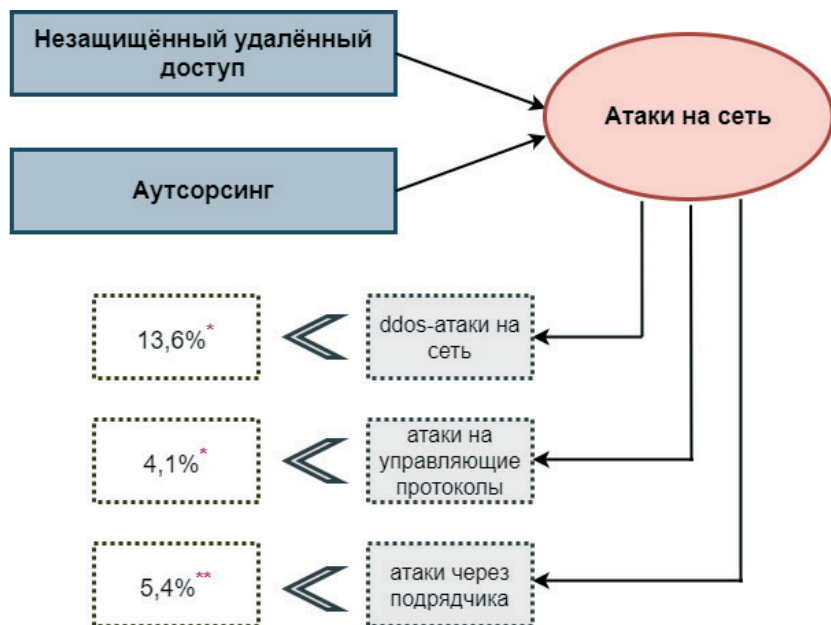
«Удалёнка», в свою очередь, «открыла» для хакеров новые возможности: незащищённые домашние сети, незакрытые корпоративные ресурсы, бесконтрольный доступ пользователей во внешние сети привели к тому, что злоумышленники стали находить новые «лазейки» для проникновения в контролируемую инфраструктуру в обход систем защиты. Случалось и так, что информационные системы, в которые проникал вирус, были защищены, но обнаружить вирус удавалось только после его разрушающего воздействия.

К основным причинам атак на сеть можно отнести следующее:

- незащищённый удалённый доступ – желание организовать удалённый доступ побыстрее и подешевле приводит к возникновению ошибок в настройке сетевых параметров и появлению уязвимостей в системе защиты сетевого окружения;
- делегирование обязанностей подрядным организациям (аутсорсинг¹⁾) – выбирая подрядные организации, компании прежде всего думают о минимизации затрат и не задумываются об обеспечении подрядчиками собственной информационной безопасности.

Наиболее распространённые виды атак на сеть и их процентное соотношение к общему количеству атак⁴⁾ отображено на рисунке 2:

¹⁾ Отчет Solar JSOC Security Report. Итоги года (https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf).



* - соотношение атак к общему количеству внешних атак на ИС (из отчета компании "Ростелеком-Солар");

** - соотношение атак к общему количеству внутренних атак на ИС (из отчета компании "Ростелеком-Солар").

Рисунок 2 - Распространённые атаки на сеть

Примечание. О том, как защитить удалённый доступ, написано в подразделе 4.1.

Многие действия сотрудников сами по себе оказываются факторами, способствующими проведению кибератак. Ряд из них характерен именно для удалённого доступа. Это, например, бесконтрольный доступ в Интернет в условиях удалённой работы (ограничить возможность выхода во внешние сети сотрудников с личных компьютеров практически невозможно).

А есть такие, что одинаковы для всех сотрудников, независимо от того, удалённо или локально они работают. Примеры такого фактора – бесконтрольные действия пользователей – описаны далее в п.п. 2.2.

2.2 БЕСКОНТРОЛЬНЫЕ ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ

К сожалению, удар может быть нанесён не только извне, но и изнутри компании. Непосредственные пользователи и сотрудники организации могут совершать умышленно или случайно действия, которые способствуют реализации угроз безопасности системы.

Сотрудники, имеющие доступ к корпоративной информации или любой другой информации конфиденциального характера и объектам инфраструктуры организации, также могут быть нарушителями¹⁾. Большинство «противоправных» действий совершается пользователями из-за отсутствия должного уровня контроля за работой сотрудников и использованием личных устройств и сервисов. В последнее время участились случаи утечки информации, компрометации внутренних учётных записей, нарушения политик доступа во внешние сети (Интернет), использования вредоносных утилит и несогласованных действий подрядных организаций, приводящих к простоям объектов КИИ – всё это следствия действий, которые выполнены обычными пользователями, иными словами, своими же сотрудниками.

Одни пользователи, в страхе потерять рабочее место из-за пандемии, сознательно выносят корпоративную информацию за пределы контролируемой зоны (на всякий случай, чтобы оставить себе какие-то ресурсы на случай потери работы), несмотря на орг.меры и требования политики безопасности.

Другие, которых можно определить, как мотивированных внутренних нарушителей, умышленно совершают злонамеренные действия, направленные против организации, в которой они сами же и работают – крадут информацию с целью дальнейшей её продажи конкурентам, умышленно внедряют в систему вредоносные программы, выводят из строя оборудование и т.д.

Третьи – обычные пользователи, которые ничего плохого не замышляют, но не задумываются о последствиях своих действий: забывают обновлять программное обеспечение на своих компьютерах, не задумываются о защите своих «домашних» рабочих мест от посторонних лиц, забывают про требования политики безопасности, пользуются личными флешками и публичными сервисами. На непроверенных устройствах вполне возможно привнести в информационную систему организации вредоносную программу. Публичные сервисы также подвержены атакам, например, по причине их некорректной конфигурации. Масса информации выносится за пределы контролируемой зоны организации на личных флешках сотрудников с вытекающими из этого последствиями – кража или потеря информации.

Примеры бесконтрольных действия и к чему они могут привести показаны на рисунке 3.

¹⁾ Ежегодный отчет Solar JSOC Security Report (<https://rt-solar.ru/analytics/reports/2135/>).

Пользователи



могут бесконтрольно



К чему эти действия могут привести:



1. Утечка информации (по данным "Ростелеком-Солар" - 53,4% от общего количества внутренних инцидентов).
2. Компрометация внутренних учётных записей (по данным "Ростелеком-Солар" - 12,3% от общего количества внутренних инцидентов).
3. Нарушение политик доступа во внешние ИС (по данным "Ростелеком-Солар" - 11,4% от общего количества внутренних инцидентов).
4. Несанкционированная активность в рамках удалённого доступа (по данным "Ростелеком-Солар" - 3% от общего количества внутренних инцидентов).

Рисунок 3 - Бесконтрольные действия пользователей и их последствия

Примечание. Как контролировать работу пользователей и ПО описано в подразделе 4.3.2.

2.3 РАЗВИТИЕ ИНСТРУМЕНТАРИЯ ЗЛОУМЫШЛЕННИКОВ

Развитие различных видов вредоносного программного обеспечения (ВрПО), в частности программ-шифровальщиков, рост атак на перехват управления, атак через цепочку поставки, взлом веб-приложений через уязвимости¹⁾ – всё это является показателем непрерывного совершенствования и усложнения инструментария злоумышленников. Как говорится, «враг не дремлет».

Совершенствуясь в подборе инструментов и придумывая новые сложные схемы проведения атак, злоумышленники становятся способны проводить не только рядовые, но и сложные атаки с применением новейших интеллектуальных технологий – от взлома роутеров домашних сетей пользователей до кражи денежных средств до счетов банков и хищения конфиденциальной информации в государственных структурах.

Ожидание в режиме самоизоляции во время пандемии, а также желание пользователей найти больше информации о коронавирусе, его последствиях и вакцине спровоцировали активизацию деятельности мошенников с применением методов социальной инженерии (среди которых лидирует фишинг⁶⁾). В поисках ответов на интересующие вопросы пользователи все чаще стали «попадаться на удочки» – специальные рассылки, подготавливаемые злоумышленниками. Пользователь переходит по ссылке, а дальше всё просто – от лица легитимного ресурса или организации мошенники предлагают пользователю авторизоваться, используя свою учётную запись. После ввода данные попадают напрямую к злоумышленникам, которые используют их для кражи корпоративной информации или денежных средств.

Примечание. Решения для защиты от вредоносного инструментария описаны в подразделе 4.3.1.

Защита от вредоносного инструментария достигается за счёт:

- обеспечения доверенной вычислительной среды как в физических инфраструктурах, так и в виртуальных;
- блокировки уязвимостей используемых приложений и средств вычислительной техники (СВТ);
- контроля неизменности вычислительной среды;
- разграничения доступа к ресурсам системы.

Распространённые виды ВрПО и способы защиты от него показаны далее на рисунке:

¹⁾ Ежегодный отчет Solar JSOC Security Report (<https://rt-solar.ru/analytics/reports/2135/>).

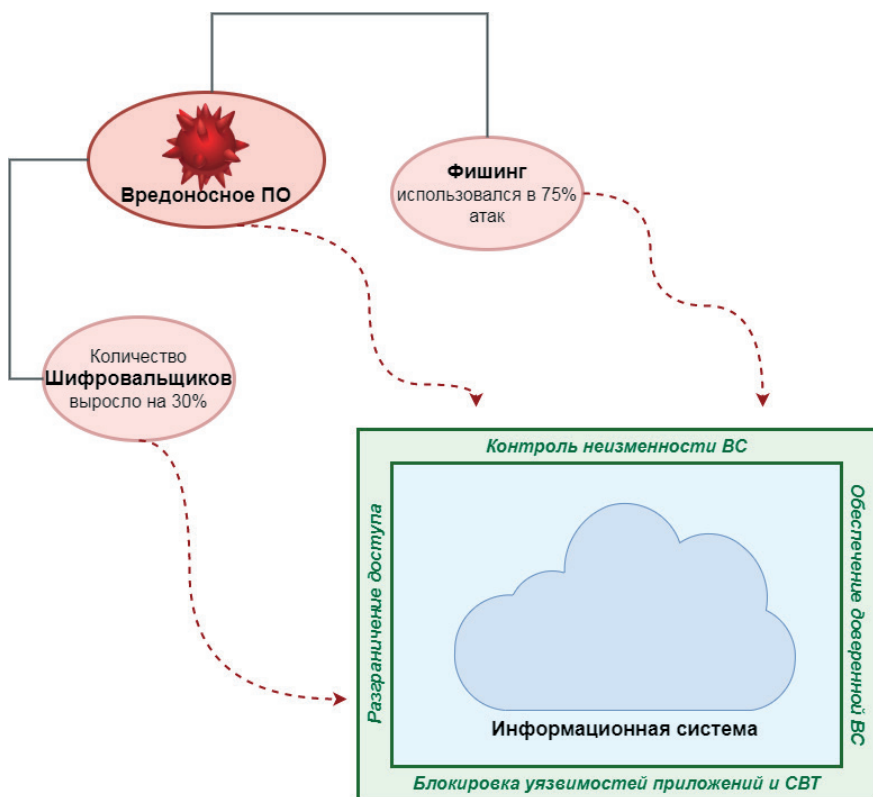


Рисунок 4 – Как защититься от вредоносного ВрПО

2.4 ДЕЛЕГИРОВАНИЕ ЗАДАЧ ПОДРЯДНЫМ ОРГАНИЗАЦИЯМ (АУТСОРСИНГ)

Аутсорсинг как явление возник довольно давно. Передача обязанностей по выполнению каких-либо функций другим организациям (подрядчикам) сокращает расходы на оборудование, аренду помещений и персонал. В информационной среде аутсорсинг широко распространён.

Прибегая к услугам подрядных организаций, компании не задумываются о том, корректно ли организуют подрядчики защиту своих собственных информационных границ. Помимо этого, сами же многие компании не проводят регулярный аудит информационной безопасности, и после прекращения сотрудничества с каким-либо подрядчиком забывают защищать ранее используемые точки доступа, что приводит к возникновению незащищённых узлов. С помощью таких «белых пятен» злоумышленники и совершают атаки. С этим связано учащение случаев проведения атак через

подрядчиков (типа Supply Chain¹⁾, которую используют, чаще всего, профессиональные киберпреступники при взломах сетей правительственных организаций).

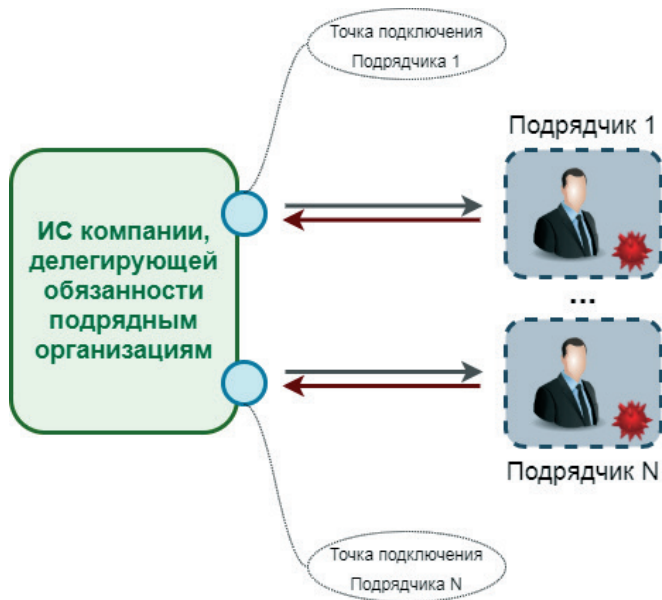


Рисунок 5 - Сетевое взаимодействие с подрядными организациями

Примечание. О том, как контролировать сторонние подключения, – в подразделе 4.2.

2.5 КИБЕРАТАКИ И СПОСОБЫ ИХ ОТРАЖЕНИЯ

Как было показано ранее, основными причинами роста числа кибератак являются:

1. незащищённый удалённый доступ;
2. пользование услугами подрядных организаций (аутсорсинг);
3. усложнение инструментария злоумышленников;
4. бесконтрольная деятельность пользователей.

Примеры действий и процессов, которые могут повлиять на рост числа кибератак, показаны на рисунке 6. Так, например, некорректная организация удалённого доступа и послабление контроля за работой пользователей в условиях удалённого доступа могут привести к возникновению уязвимостей в структуре сетевого окружения, что, в свою

¹⁾ Отчет Solar JSOC Security Report. Итоги года (https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf).

очередь, является благоприятным условием для совершения сетевых атак. Другой пример, развитие разновидностей вредоносного ПО и отсутствие контроля за обновлением ПО пользовательских компьютеров определяют возникновение уязвимостей в структуре информационной системы – увеличивается риск атаки на инфраструктуру.

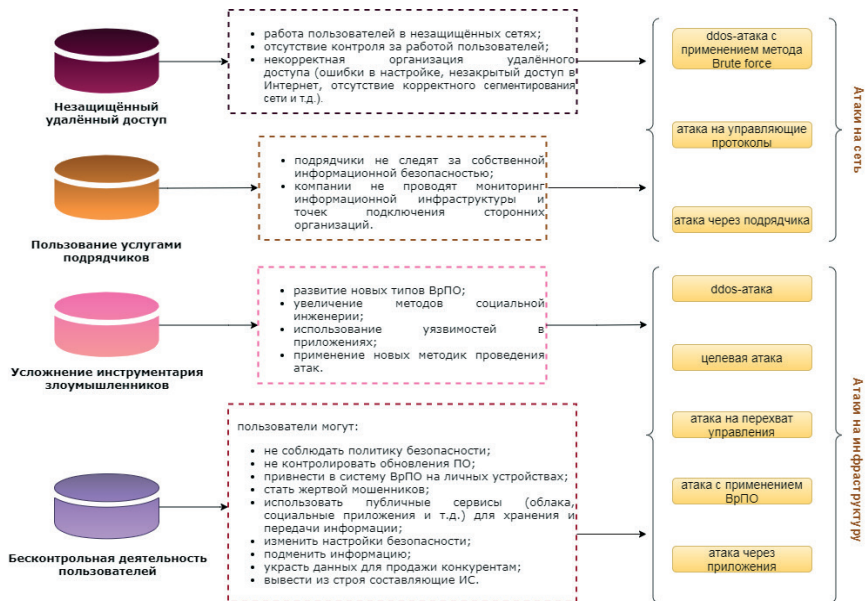


Рисунок 6 - Последствия роста числа кибератак

Подобная картина вызывает объяснимые сомнения в том, что кибератаки вообще возможно отразить без заметного ущерба для информационных ресурсов.

Защитить информационную систему от потенциальных кибератак возможно.

3 ЗАЩИТА ОТ КИБЕРАТАК

Разумный способ обеспечить безопасность информационной системы заключается в применении многосторонней защиты: необходимо не только защитить элементы инфраструктуры, но и организовать корректное взаимодействие сотрудников и применяемого программного обеспечения, т.е. контролировать процессы и управлять доступом пользователей к корпоративным ресурсам.

Ни для кого не секрет, что для обеспечения эффективной защиты компьютеров и сетевой инфраструктуры необходимо применить специальные средства защиты информации, коих, к счастью, на сегодняшний день существует множество.

Как определиться с выбором и среди массы вариантов выбрать надёжные продукты?

Надёжные и качественные решения защиты информационной среды должны защитить ИС от кибератак:

- защитить удалённый доступ;
- контролировать точки подключения сторонних организаций;
- противодействовать инструментам злоумышленников – контролировать инфраструктуру;
- контролировать работу пользователей и ПО.

Способы защиты от различных типов кибератак показаны далее в таблице 1.

Таблица 1 - Противодействие кибератакам

Типы кибератак	Причины роста числа кибератак	Способы защиты
Атаки на сеть	Незащищённый удалённый доступ	Защита удалённого доступа: ✓ контроль сетевой инфраструктуры; ✓ обеспечение непродолжительного защищённого доступа пользователя доступа к корпоративным ресурсам (доверенного сеанса связи); ✓ контроль точек подключения сторонних организаций – контроль сетевой инфраструктуры; ✓ антивирусная защита.
Атаки на инфраструктуру	Усложнение инструментария злоумышленников	Защита и контроль инфраструктуры: ✓ обеспечение доверенной вычислительной среды;
	Пользование услугами	

	сторонних организаций	✓ блокировка уязвимостей используемых приложений и средств вычислительной техники (СВТ); ✓ контроль неизменности вычислительной среды; ✓ контроль целостности настроек, в том числе собственных; ✓ централизованное управление настройками и работой пользователей; ✓ контроль за работой установленного на компьютерах пользователей программного обеспечения (ПО); ✓ разграничение доступа; ✓ мониторинг событий ИБ; ✓ контроль обновлений ПО; ✓ мониторинг событий ИБ; ✓ использование специальных защищённых носителей информации; ✓ применение специальных инструментов для управления встроенными механизмами безопасности.
	Бесконтрольная деятельность пользователей	

В большинстве случаев для комплексной защиты структуры ИС необходимо применять не одно, а совокупность средств защиты – для блокировки нескольких угроз безопасности, связанных с несколькими факторам возникновения кибератак.

Немаловажно выбранные средства увязать между собой. Необходимо, чтобы в процессе эксплуатации интегрированные решения функционировали неизменно и слаженно, не блокируя работу друг друга. Стабильно функционирующая система – менее уязвимая система.

Не секрет, что самыми приемлемыми по части согласованности и увязке являются решения одного производителя.

Кроме того, рекомендованным вариантом являются решения отечественного производства, на которые (и на составные части которых) имеются сертификаты¹⁾.

Возможно ли в принципе собрать систему защиты от актуальных кибератак из отечественных продуктов так, чтобы система реально работала без сбоев, и при этом соответствовала требованиям регуляторов?

¹⁾ Даже если сертификатов нет, то получить их не так затруднительно, чем на зарубежные средства.

4 РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

ОКБ САПР располагает множеством различных категорий продуктов с безупречной репутацией.

Каждый отдельный продукт обладает уникальным набором функций и возможностей, но при этом совместим с другими решениями, что позволяет обеспечивать комплексную защиты ИС организаций-заказчиков и преобразовывать их в единый слаженный защищённый механизм с минимальными затратами по интеграции и настройке.

Рассмотрим категории продуктов ОКБ САПР, способных противостоять кибератакам и предотвратить их последствия, а также их основные способы защиты:

Каждый отдельный продукт обладает уникальным набором функций и возможностей, но при этом совместим с другими решениями, что позволяет обеспечивать комплексную защиты ИС организаций-заказчиков и преобразовывать их в единый слаженный защищённый механизм с минимальными затратами по интеграции и настройке.

Рассмотрим категории продуктов ОКБ САПР, способных противостоять кибератакам и предотвратить их последствия, а также их основные способы защиты:

- средства защиты удалённого доступа (п.п. 4.1):
 - средство обеспечения доверенного сеанса (СОДС) «МАРШ!»;
 - «TrusT Удалёнка»;
 - двухконтурный моноблок;
 - защищённые терминалы «m-TrusT Терминал» и «Центр-TrusT»;
 - криптошлюзы «fin-TrusT»;
 - TrusT-in-Motion;
- средства контроля точек подключения сторонних организаций (п.п. 4.2):
 - МЭ «TrusT»;
- средства контроля информационной инфраструктуры (п.п. 4.3):
 - средства защиты от вредоносного инструментария:
 - ✓ средства доверенной загрузки:
 - средство защиты от несанкционированного доступа (СЗИ от НСД) «Аккорд-АМДЗ»;
 - СЗИ от НСД «ИНАФ»;
 - средство доверенной загрузки (СДЗ) «Аккорд-МКТ»;
 - ✓ средства защиты систем виртуализации (специальное программное обеспечение (СПО) «Аккорд-KVM», СПО «Аккорд-В.», СПО «Сегмент-В.»);
 - ✓ защищённые микрокомпьютеры m-TrusT;
 - ✓ средства разграничения доступа (программно-аппаратный комплекс «Аккорд-Х», СПО «Аккорд-Win64 К», СПО «Аккорд-Х К»);

- средства контроля за работой пользователей:
 - ✓ средства централизованного управления:
 - ПАК «Центр-Т»;
 - автоматизированное рабочее место (АРМ) защищенного хранения и сетевой загрузки на базе микрокомпьютера «m-TrusT»;
 - система удалённого централизованного управления «Аккорд» («СУЦУ»);
 - программный продукт (ПП) «Паспорт ПО»;
 - ✓ защищённые носители информации:
 - семейство защищенных съемных носителей: ПАК «Секрет Особого Назначения», ПАК «Секрет Фирмы», ПАК «Секрет Администратора»;
 - носители ключевой информации (ПАК «Идеальный токен»);
 - средства архивирования журналов (ПАК «ПАЖ»);
 - отчуждаемый шлюз (ПАК «Система Ниппель»);
- специальные инструменты для управления встроенными механизмами безопасности:
 - ✓ USB Guard. Функциональный модуль UEFI.

Один из способов защиты информационных ресурсов компании с применением средств защиты удалённого доступа, контроля точек подключения подрядных организаций и контроля информационной среды, разработанных ОКБ САПР, показан на рисунке 7.

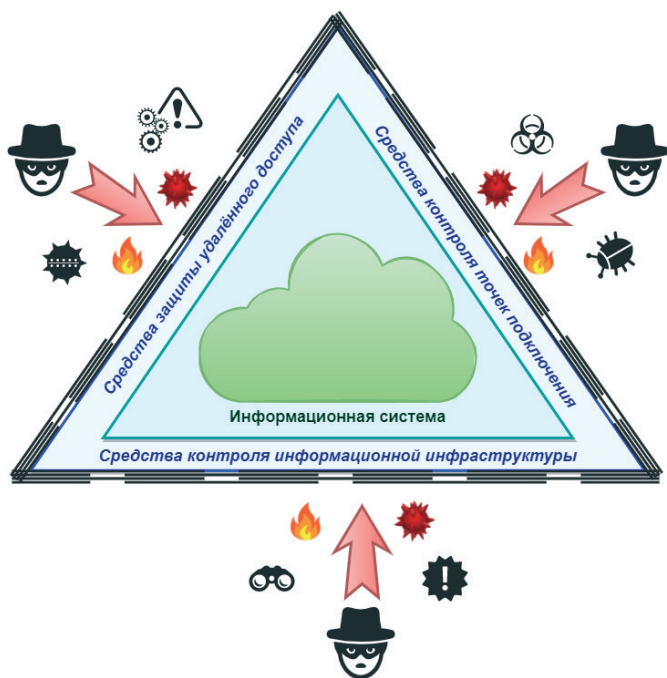


Рисунок 7 - Решения для защиты информационных ресурсов ОКБ САПР

Далее о продуктах.

4.1 СРЕДСТВА ЗАЩИТЫ УДАЛЁННОГО ДОСТУПА

Как уже говорилось в п.п. 2.1 к основным причинам атак на сеть можно отнести следующее:

- незащищённый удалённый доступ;
- делегирование обязанностей подрядным организациям (аутсорсинг¹⁾).

Компанией ОКБ САПР разработаны различные средства защиты удалённого доступа. Одни решения позволяют работать в доверенной среде короткий промежуток времени, их можно переносить и использовать только тогда, когда необходимо выполнить какие-либо действия с защищённым удалённым ресурсом, другие – организуют доверенную вычислительную среду, устанавливаются стационарно на СВТ (либо уже являются защищёнными СВТ).

¹⁾ Отчет Solar JSOC Security Report. Итоги года (https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf).

ОКБ САПР предлагает несколькими категориями продуктов, обеспечивающих защиту удалённого доступа:

- отчуждаемые средства обеспечения доверенного сеанса связи, выполненные по технологии USB-носителя («МАРШ!» и «М!&М», описании которых см. далее в данном подразделе);

- средства защиты и защищенные СВТ на базе специализированного микрокомпьютера с аппаратной защитой данных m-TrusT:

- защищенные СВТ (специальное средство вычислительной техники для удалённого доступа «TrusT Удалёнка», двухконтурный моноблок, защищенные терминалы «m-TrusT Терминал» и «Центр-TrusT», подробнее о которых можно узнать в п.п. 4.1.2, 4.1.3, 4.1.4);

- средства защиты сетевого взаимодействия (семейство криптошлюзов «fin-TrusT», маршрутизатор TrusT-in-Motion, межсетевой экран МЭ-TrusT, подробнее – в п.п. 4.1.5, 4.1.6, 4.2.1).

Объединяет данные категории решений наличие «вирусного иммунитета» к любым типам вредоносного ПО и невозможность совершения атаки на перехват управления.

4.1.1 СОДС «МАРШ!» и «М!&М»

Практика показывает, что организация ДВС на компьютерах пользователей, которые в рамках должностных обязанностей работают с удалённой защищённой системой непродолжительное время, неуместна – стоимость ДВС высока, а организация сложна.

Для кратковременного соединения с защищённой корпоративной сетью рациональнее использовать средства доверенного сеанса связи (ДСС), которые организуют доверенную среду на некоторое время.

СОДС «МАРШ!»¹⁾ организует ДСС с удалённой системой, в рамках которого поддерживается доверенная среда.

Устройство подключается к незащищённому компьютеру, загружает на него ОС из защищённой от перезаписи памяти и устанавливает защищённое соединение с удалённой информационной системой.

На этапе производства память СОДС «МАРШ!» разбивается на разделы и к ним устанавливаются различные права доступа, которые контролируются микроконтроллером и пользователем изменены быть не могут:

¹⁾ СОДС «МАРШ!» (<https://www.okbsapr.ru/products/storage/compute/sods/>).

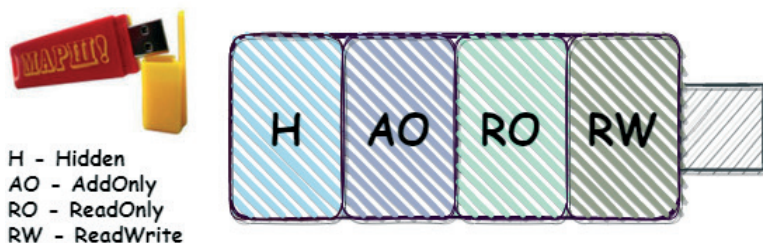


Рисунок 8 – Структура памяти СОДС «МАРШ!»

Как правило, память СОДС «МАРШ!» содержит не менее одного раздела ReadOnly (RO), не менее одного раздела ReadWriteHidden (RWH), используются также разделы AddOnly (AO) и разделы с общим доступом RW.

В RO разделе размещаются ОС и другое ПО, которое является неизменяемым достаточно длительное время. Обновления и дополнения функционального ПО обычно размещаются в одном из разделов RWH, в другом размещается ключевая информация VPN, а раздел AO используется для ведения аппаратных журналов событий безопасности.

В рамках ДСС между собой взаимодействуют Клиент ДСС и Сервер ДСС.

В качестве Клиента ДСС выступает компьютер пользователя, загруженный с СОДС «МАРШ!». Вне зависимости от варианта исполнения в рамках ДСС СОДС «МАРШ!» обеспечивает:

- доверенную загрузку ОС;
- защищённое соединение с Сервером ДСС на основе асимметричных криптографических алгоритмов;
- возможность использования устройства «МАРШ!» в качестве средства идентификации-аутентификации пользователя для доступа к сервисам РИС (в т. ч. хранение ключей и сертификатов);
- среду функционирования ПО для подготовки и обработки данных;
- среду функционирования прикладного ПО сторонних производителей.

Сервер ДСС – это доверенный сервер, обеспечивающий:

- организацию защищенного соединения с Клиентом ДСС и Сервером авторизации РИС;
- авторизацию пользователя Клиента ДСС на доступ к сервисам РИС;
- организацию защищенной работы пользователя Клиента ДСС с сервисами РИС в рамках ДСС.

Для начала доверенного сеанса пользователь загружается с «МАРШ!», обеспечивая тем самым доверенную среду.

Органы управления загруженной ОС недоступны пользователю, рабочая среда полностью изолирована от посторонних сетевых соединений, открытый трафик отсутствует, сеанс связи завершается после завершения работы в браузере.

После запуска ОС стартует браузер и все сопутствующее ПО, необходимое для работы.

После старта браузера устанавливается доверенный сеанс связи с сервером ДСС. Сервер информационной системы выполняет авторизацию пользователя на доступ к сервисам информационной системы и соединение с требуемым сервисом.

«МАРШ!» – это «серебряная пуля» для хакера, поскольку

- состояние критичных компонентов зафиксировано,
- вирусы блокированы,
- ключи неизвлекаемы,
- перехват управления невозможен,
- управление отчуждено от клиента (пользователь не может ничего напороть).

Вариант «М!&М» отличается от СОДС «МАРШ!» наличием модуля связи в качестве встроеного аппаратного компонента (рисунок 9).

При необходимости организации ДСС с рабочего мобильного места, у которого нет собственных средств связи, более предпочтительным вариантом является использование модема.

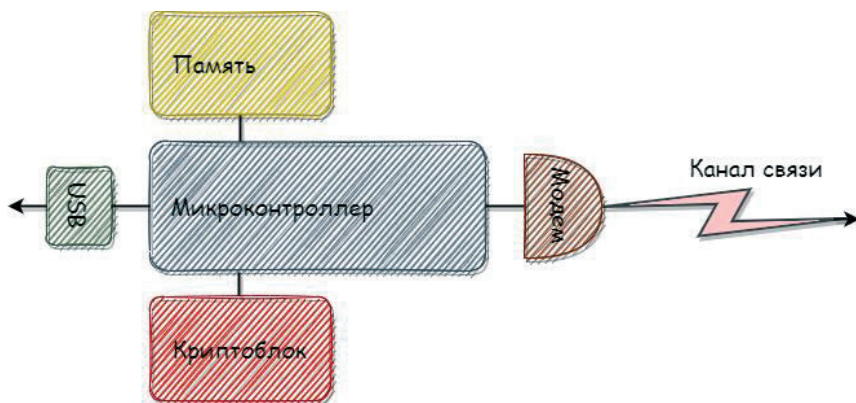


Рисунок 9 - Вариант «М!&М»

Такой вариант подходит, например, для удаленной работы сотрудника банка, оформляющего банковские карты. Многие банки предлагают оформление карты в любом удобном для клиента месте, а иногда этот способ оформления карты – единственно возможный (для интернет-банков).

При использовании «М!&М»¹⁾ можно быть уверенным в том, что никакое несанкционированное воздействие не сможет изменить программное обеспечение устройства, а значит, и повлиять на прием и передачу данных.

¹⁾ М!&М (<https://www.okbsapr.ru/products/storage/compute/sods/m-m/>).

Здесь стоит отметить, что при загрузке с СОДС «МАРШ!» не выполняется требование УПД.17, так как при загрузке с флешки не проводится контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники. Данное обстоятельство затрудняет организацию защиты удалённого доступа в ГИС первого класса. Эта задача не решается с помощью традиционно предлагаемых в качестве решения для удалённого доступа средств хранения и загрузки на компьютер ОС с защищенного тем или иным образом носителя на базе USB-накопителя. Даже в тех случаях, когда, согласно рекламным материалам, микроконтроллер этого устройства загружается доверенным образом, это никак не связано с УПД.17, так как в этом требовании говорится о контроле целостности СБТ, а не носителя ОС.

Для решения такой задачи ОКБ САПР разработала специальное средство защиты – ССБТ УД «TrusT Удалёнка», о котором далее и пойдёт речь.

4.1.2 «TrusT Удалёнка»

«TrusT Удалёнка»¹⁾ – это специальное средство вычислительной техники, предназначенное для организации защищённого контролируемого удалённого доступа в государственных информационных системах (ГИС). В состав ССБТ УД «TrusT Удалёнка» входит СКЗИ, сертифицированное ФСБ по классу КСЗ.

Аппаратная платформа ССБТ УД представляет собой защищенный микрокомпьютер, архитектура которого обеспечивает невозможность воздействия вредоносного ПО на ССБТ УД. Благодаря наличию встроенного СКЗИ обеспечивается удалённое защищенное соединение с ГИС. Входящее в состав СДЗ в совокупности со специальным средством разграничения доступа обеспечивают доверенную загрузку ОС ССБТ УД и блокировку доступа неавторизованных пользователей к ресурсам ГИС. Помимо этого, в ССБТ УД имеется встроенный браузер, что позволяет получить безопасный доступ к различным интернет-сервисам.

Схема работы при использовании ССБТ УД «TrusT Удалёнка» следующая: к компьютеру пользователя подключен микрокомпьютер.

При необходимости подключения к ГИС, с него на компьютер пользователя загружается технологическая ОС с терминальным клиентом, и микрокомпьютер становится для компьютера пользователя терминальным сервером.

¹⁾ TrusT Удалёнка (<https://www.okbsapr.ru/products/newharvard/trust-udalyenka/>).

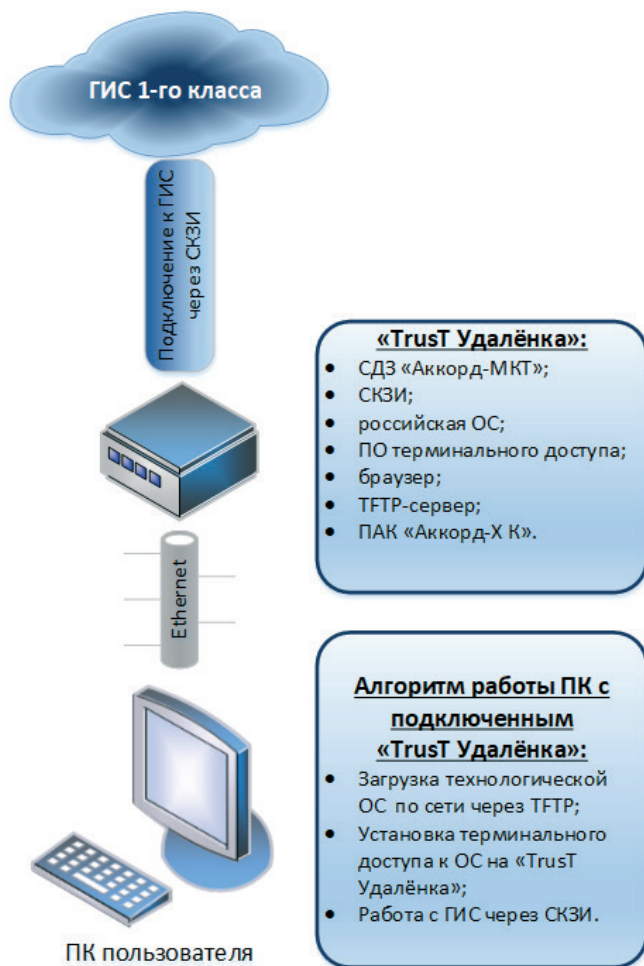


Рисунок 10 - Схема работы при использовании ССВТ УД «TrusT Удалёнка»

На компьютере выполняется:

- PXE-загрузчик, интегрированный в BIOS;
- технологическая ОС, загружаемая с «TrusT Удалёнка»;
- ПО терминального клиента (в ОС, загруженной с «TrusT Удалёнка»);

На «TrusT Удалёнка» выполняется:

- СДЗ уровня BIOS Аккорд-МКТ (сертифицированное ФСТЭК России);
- российская ОС, в том числе:

- ПО терминального сервера (навстречу ПЭВМ);
- ПО терминального клиента (навстречу ГИС);
- драйвера сети;
- браузер;
- TFTP-сервер (поддержка загрузки по PXE);
- «Аккорд-Х К» (для изоляции программной среды по требованиям ФСБ России, сертифицирован ФСТЭК России);
- СКЗИ DCrypt (сертифицирован ФСБ России на платформе m-TrusT на класс КСЗ).

При применении ССВТ УД выполняется требование УПД.17 в отличие от СОДС «МАРШ!» см. п.п. 4.1.2), что важно при организации защиты удалённого доступа в ГИС первого класса.

Здесь следует упомянуть, что требование УПД.17 «Доверенная загрузка средств вычислительной техники» выполняется, если обеспечиваются:

- недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;
- контроль доступа пользователей к процессу загрузки операционной системы;
- контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

При загрузке с «TrusT Удалёнка» описанные выше условия обеспечения требования УПД.17 выполняются за счет:

- контроля целостности программного обеспечения и аппаратных компонентов именно того средства вычислительной техники, на котором исполняется СКЗИ (посредством встроенного СДЗ уровня BIOS «Аккорд-МКТ»).

- входящего в состав ССВТ УД микрокомпьютера m-TrusT, память которого находится в режиме «только чтение»: при загрузке команды и данные размещаются в сеансовой памяти, в которой и исполняются, то есть в случае проникновения вирусного ПО в ОС микрокомпьютера, зафиксироваться в памяти оно не сможет, что исключает возможность модификации защищаемых ресурсов при загрузке нештатной ОС.

Встроенный ПАК «Аккорд-Х К» контролирует целостность исполняемой ОС.

Также за счет реализации в «m-TrusT» функции неизвлекаемого ключа, возможно использовать ключ до 3-х лет.

Одновременно не требуется дополнительный ключевой носитель и меры по контролю этих носителей, поскольку ключи хранятся на самом устройстве в неизвлекаемом виде.

При использовании «TrusT Удалёнка» нагрузка на пользователя минимальна. К тому же стоимость подготовки клиентского рабочего компьютера гораздо ниже, чем при использовании подготовленных стационарных устройств.

4.1.3 Двухконтурный моноблок

Двухконтурный моноблок¹⁾ – это, собственно, моноблок, позволяющий пользователю работать в одной из двух защищенных ОС (в общем случае одна из них Windows, а вторая – Linux) (см. рис. 12).



Рисунок 11 – Двухконтурный моноблок

– ОС Windows загружается с жесткого диска моноблока. При работе в этом режиме пользователь может устанавливать любое ПО и инициировать любые подключения в рамках заданных для него правил разграничения доступа: в ОС установлено СПО «Аккорд-Win64 К», и при необходимости выполнения контрольных процедур до или во время работы пользователя администратор может произвести соответствующую настройку комплекса.

– СПО «Аккорд-Win64 К» может быть установлено совместно со средством доверенной загрузки (СДЗ), так и без него. Вариант установки СПО зависит от пожеланий Заказчика. В общем случае возможны следующие варианты применения СПО «Аккорд-Win64 К»:

- без средства доверенной загрузки;
- с СДЗ уровня BIOS (СПО «Аккорд-МКТ»);
- с СДЗ уровня платы расширения (комплексом «Аккорд-АМДЗ»).

В случае применения СПО «Аккорд-Win64 К» без СДЗ обеспечивается защита информации в авторизированных системах до 1Г класса защищенности включительно, также обеспечивается соответствие 4 уровню доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий.

При использовании СПО «Аккорд-Win64 К» с СДЗ обеспечивается защита информации в авторизированных системах до 2А и 2Б класса защищенности, а также обеспечивается соответствие 2 уровню доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий.

При запуске Двухконтурного моноблока во втором режиме ОС Linux загружается из защищенного от записи раздела памяти микрокомпьютера «m-TruST», то есть не просто с другого жесткого диска, а с другого компьютера. При работе в этом режиме пользователю доступно только ПО для доступа к терминальному серверу и дополнительное ПО, необходимое для работы в рамках терминальной сессии.

Принципиальное отличие этого решения от решений на базе подключаемых носителей доверенной среды состоит в том, что моноблок не мобилен, но при этом предоставляет пользователю две полнофункциональные среды, а не только защищенный

¹⁾ Двухконтурный моноблок (<https://www.okbsapr.ru/products/newharvard/Dvukhkconturnyymonoblok/>).

доступ к некоторой системе, при этом работа в этих средах может вестись параллельно, а не последовательно, для переключения не требуется ни перезагрузка, ни смена сеанса, все процессы продолжают в каждой ОС своим чередом.

Архитектура микрокомпьютера «m-TrusT» обеспечивает высокий уровень вирусного иммунитета. Высокий уровень конфиденциальности и доверенная среда функционирования криптографии обеспечивается за счет встроенного РКБ.

Наличие в «m-TrusT» встроенного СДЗ уровня BIOS (СПО «Аккорд-МКТ») обеспечивает доверенную загрузку ОС. Использование СЗИ НСД (СПО «Аккорд-Х К») обеспечивает разграничение доступа пользователей, а также регистрацию событий, контроль целостности и контроль подключения машинных носителей.

4.1.4 Защищённые терминалы «m-TrusT Терминал» и «Центр-TrusT»

Защищённый терминал на базе микрокомпьютера m-TrusT представляет собой СВТ в едином корпусе, предназначенное для организации защищённого канала передачи данных при подключении к терминальным серверам обработки данных в критических информационных структурах¹⁾.



Рисунок 12 – «m-TrusT Терминал»

Варианты реализации защищенного терминала различаются способом организации хранения и загрузки ОС:

- первый вариант – ОС полностью хранится в памяти микрокомпьютера, доступной в режиме «только чтение». Такой вариант реализации защищенного терминала называется «m-TrusT Терминал»;

- второй вариант – в переменную часть выделяется не только конфигурация, но и некий набор функционального ПО, которое не может располагаться в неизменяемой памяти. В этом случае загружаться переменная часть образа ОС может по технологии

¹⁾ Защищённые терминалы m-TrusT Терминал и Центр-TrusT (<https://www.okbsapr.ru/products/newharvard/ZashchishchennyyterminalnabazemTrusT/>).

защищенной сетевой загрузки «Центр-Т». Такой вариант реализации защищенного терминала называется «Центр-TrusT».

Внешний вид передней панели терминала представлен далее:



Рисунок 13 - Внешний вид передней панели

- 1 – 2 USB-порта 2.0 (type A);
- 2 – индикатор состояния изделия;
- 3 – кнопка запуска изделия.

Внешний вид задней панели изделия представлен ниже:

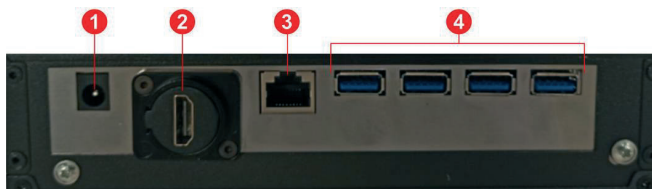


Рисунок 14 - Внешний вид задней панели

- 1 – разъем для подключения кабеля питания;
- 2 – 1 порт HDMI;
- 3 – 1 Gbps Ethernet-порт (RJ45);
- 4 – 4 USB-порта 3.0 (type A).

Функциональность защищённого терминала такова, что пользователь может работать на нем, как на обычном ПК, но при этом посредством криптографических механизмов обеспечивается защита критичной информации и высокий уровень вычислительной мощности.

Защищённый терминал на базе микрокомпьютера m-TrusT построен на базе Новой гарвардской архитектуры, что обеспечивает высокий уровень вирусного иммунитета. Встроенный резидентный компонент безопасности создаёт доверенную среду функционирования криптографии и позволяет поддерживать высокий уровень конфиденциальности. Подключение к серверам обработки данных по защищенному каналу связи и использование встроенного аппаратного блока неизвлекаемого ключа обеспечивает простоту использования с соблюдением всех требований регулятора.

Наличие встроенного ПО «Аккорд-МКТ» и «Аккорд-Х К» обеспечивает доверенную загрузку ОС и разграничение доступа пользователей, а также регистрацию событий, контроль целостности и контроль подключения машинных носителей.

Аппаратная платформа терминала имеет производительный процессор – RK3399, совместима с последними версиями ядра Linux и поддерживает интерфейсы USB 3.0 и USB Type-C, что обеспечивает высокий уровень вычислительной мощности при относительно низком энергопотреблении.

Ресурсы терминала позволяют обеспечить среду функционирования криптографии, позволяющую сертифицировать вариант исполнения СКЗИ (может быть различным) на m-TrusT на класс КСЗ.

Дополнительно возможны:

- реализация поддержки sd-карт;
- реализация блока защиты от инвазивных атак.

Удаленный доступ с защищенного терминала на базе m-TrusT может осуществляться с помощью встроенных средств, выбранных на этапе заказа:

- Citrix ICA;
- Virtual Network Computing (VNC)¹⁾ ;
- Free RDP.

Основная функциональность m-TrusT Терминала:

- идентификация и аутентификация пользователя;
- контроль целостности ПО;
- доверенная загрузка ОС;
- защита от несанкционированной модификации программ и данных;
- «вирусный иммунитет»;
- защита информации при ее передаче по каналам связи;
- исключение доступа через общие ресурсы;
- доверенный сеанс связи пользователя с удаленными ресурсами;
- регистрация действий пользователя.

Основная функциональность Центр-TrusT:

- идентификация и аутентификация пользователя;
- защищенная загрузка ПО по сети;
- защита от несанкционированной модификации программ и данных;
- удаленное администрирование загружаемых образов;
- «вирусный иммунитет»;
- защита информации при ее передаче по каналам связи (опционально);
- исключение доступа через общие ресурсы;
- доверенный сеанс связи пользователя с удаленными ресурсами;
- регистрация действий пользователя.

¹⁾ https://ru.wikipedia.org/wiki/Virtual_Network_Computing.

Защищённые терминалы на базе m-TrusT просты в обращении и не требуют наличия профессиональных навыков при установке и настройке. Кроме того, терминалы на базе m-TrusT находятся в доступной ценовой категории (их стоимость гораздо ниже, чем стоимость их аналогов).

4.1.5 Криптошлюзы fin-TrusT

fin-TrusT – решение на базе микрокомпьютера Новой гарвардской архитектуры m-TrusT – это криптошлюз для защиты сетевого взаимодействия технических средств финансовой организации¹⁾.

С помощью криптошлюзов fin-TrusT защищаются коммуникации между подразделениями и офисами банков, банком и процессинговым центром, процессинговым центром и банкоматами. Выполняются требования законодательства, блокируются уязвимости во взаимодействии в финансовой сфере.

Криптошлюз функционирует прозрачно для пользователя, не добавляя в его привычный набор действий никаких новых.

Встроенное по умолчанию в fin-TrusT СКЗИ – DCrypt от компании ТСС – сертифицировано ФСБ России в исполнениях на m-TrusT на классы КС2 и КС3.

Fin-TrusT на базе микрокомпьютера m-TrusT может использоваться совместно с ПАК КриптоПро NGate для организации защищенной сетевой коммуникации между элементами критической информационной инфраструктуры (КИИ).

Наличие собственной ОС и вычислительных ресурсов позволяет обеспечить достаточную для защиты сетевого взаимодействия производительность и высокий уровень защищенности. Наличие датчика случайных чисел и размещение ПО в памяти с доступом «только чтение» исключает вредоносное воздействие на ПО и обеспечивает неизменность среды функционирования СКЗИ.

Линейка fin-TrusT включает:

- «fin-TrusT банкомат» – криптошлюз в технологическом корпусе для установки в банкоматы с возможностью поддержки двух и более операторов мобильного Интернета.
- «fin-TrusT офис» – криптошлюз в корпусе одноюнитового сервера для установки в бэк- или фронт-офис до пятидесяти абонентских устройств.
- «fin-TrusT центр» – сервер VPN для установки в центр обработки данных (ЦОД) или серверную стойку головного отделения.

Fin-TrusT поддерживает одновременную работу нескольких независимых каналов связи. К примеру, могут быть подключены 2 Ethernet от различных провайдеров и/или 2 LTE-модема различных операторов связи, что повышает отказоустойчивость и является актуальной задачей именно для банкоматов.

Решения «fin-TrusT» могут поставляться в корпусе, без корпуса с различными интерфейсными платами, в виде платы-мезонина или в виде одноюнитового сервера в стойку (рисунки 15, 16, 17, 18).

¹⁾ Криптошлюз fin-TrusT (<https://www.okbsapr.ru/products/newharvard/kriptoshlyuz-fin-trust/>).



Рисунок 15 - Вариант исполнения криптошлюзов fin-Trust в корпусе

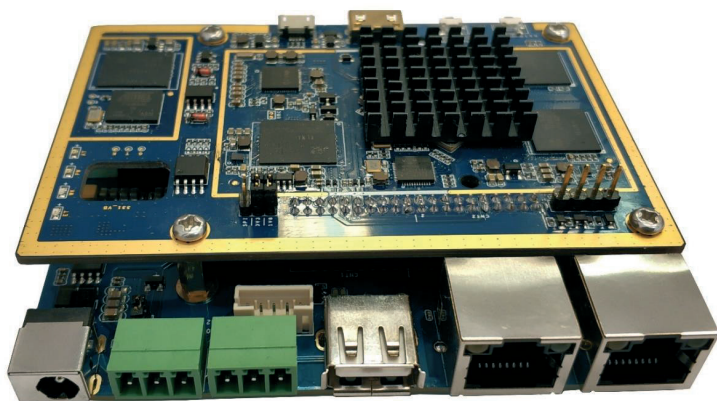


Рисунок 16 - Вариант исполнения криптошлюзов fin-Trust без корпуса с интерфейсной платой

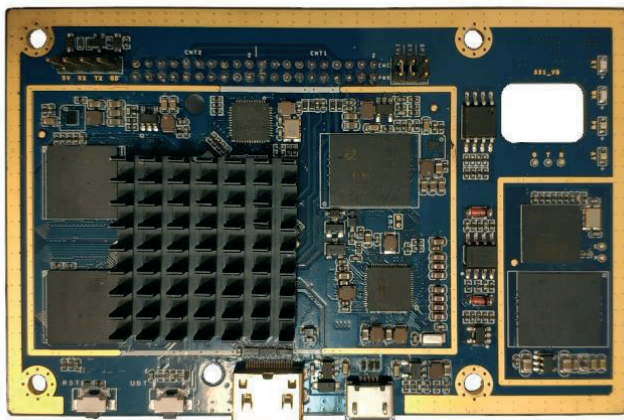


Рисунок 17 - Вариант исполнения криптошлюзов fin-TruST без корпуса в виде платы-мезонина



Рисунок 18 - Вариант исполнения криптошлюзов fin-TruST без корпуса в виде одноюнитового сервера в стойку

4.1.6 Trust-in-Motion

TrusT-in-Motion¹⁾ – это канальный шифратор для подвижных объектов КИИ (маршрутизатор), построенный на базе защищенного микрокомпьютера m-TrusT²⁾, обеспечивающий непрерывное защищённое сетевое взаимодействие в системах с подвижными объектами в условиях интенсивных вибрационных воздействий и экстремальных показателей температур.

Отличительными характеристиками маршрутизатора TrusT-in-Motion являются автоматическое включение устройства при подаче питания и наличие встроенного аппаратного блока неизвлекаемого ключа, что делает маршрутизатор пригодным для использования в средах, функционирующих без участия персонала, так как не требуется его включения, подключения носителей ключей и пр.

Такая реализация повышает стойкость маршрутизатора к интенсивным внешним воздействиям (в отличие от токенов, смарт-карт и ТМ-идентификаторов, которые ее снижают, так как на их функционирование, как правило, внешние воздействия оказывают ощутимое негативное влияние). Это очень важно для многих автоматизированных систем с подвижными объектами. Например, эти свойства определяют возможность применения маршрутизатора на беспилотных летательных аппаратах.

TrusT-in-Motion обеспечивает гибкое управление трафиком и криптографическую защиту сети. Архитектура маршрутизатора позволяет корректно функционировать, не опасаясь нарушения сетевого взаимодействия подвижных объектов системы.

Маршрутизатор TrusT-in-Motion обеспечивает бесперебойное функционирование в условиях вибрационных воздействий и изменений температуры окружающей среды: прочный металлический корпус и крепление посредством din-рейки позволяет использовать TrusT-in-Motion на движущихся объектах в температурном режиме от -40 до +80 градусов Цельсия.

Принимая потоки данных, TrusT-in-Motion выполняет их анализ и распределение, обеспечивая защиту сети. Встроенный резидентный компонент безопасности создаёт доверенную среду функционирования криптографии.

Благодаря производительному процессору RockChip RK3399 маршрутизатор обеспечивает высокий уровень вычислительной мощности при относительно низком энергопотреблении (26Вт).

TrusT-in-Motion имеет небольшие габаритные размеры – 210 x 192 x 45 мм. На внешнем корпусе имеются сетевые разъемы и разъём внешнего питания от преобразователя постоянного тока 50В на 12В (кабель питания входит в комплект поставки).

На корпусе устройства имеются два сетевых разъема. Это одна из возможных реализаций устройства, выполненная пожеланиям Заказчика.

Вместо портов Ethernet могут быть, например, USB-порты для USB-модема.

¹⁾ TrusT-in-Motion (<https://www.okbsapr.ru/products/newharvard/TrusTinMotion/>).

²⁾ <https://www.okbsapr.ru/products/newharvard/>.



Рисунок 19 - Внешний вид Trust-in-Motion. Вид сверху

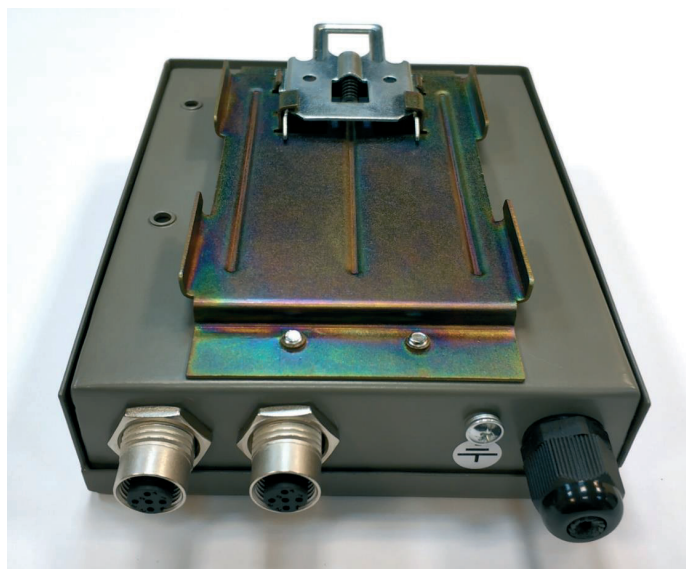


Рисунок 20 - Внешний вид Trust-in-Motion. Крепление на din-рейку

Примеры применения устройства TrusT-in-Motion

Инфраструктура сети любого транспорта состоит из стационарных (центры управления, станции (остановки)), так и подвижных объектов – поездов, автобусов, кораблей, самолетов. Далее на рисунках изображены примеры применения TrusT-in-Motion: в качестве ответной части на стационарных объектах для упрощения изображены также TrusT-in-Motion, однако, там могут быть, разумеется, как они, так и другие криптошлюзы на базе m-TrusT или других платформ, главное – с тем же СКЗИ.

1. Пример защищенного сетевого взаимодействия объектов наземного транспорта

Стационарное оборудование, размещенное в дата-центре (ЦОД), взаимодействует с оборудованием станций (остановок) и транспортных средств, например, поездов. Поезда параллельно взаимодействуют со станционным оборудованием, размещенным на станциях и в ЦОД.

Ниже на рисунке изображена организация защищенного сетевого взаимодействия объектов такой инфраструктуры с помощью маршрутизатора TrusT-in-Motion.

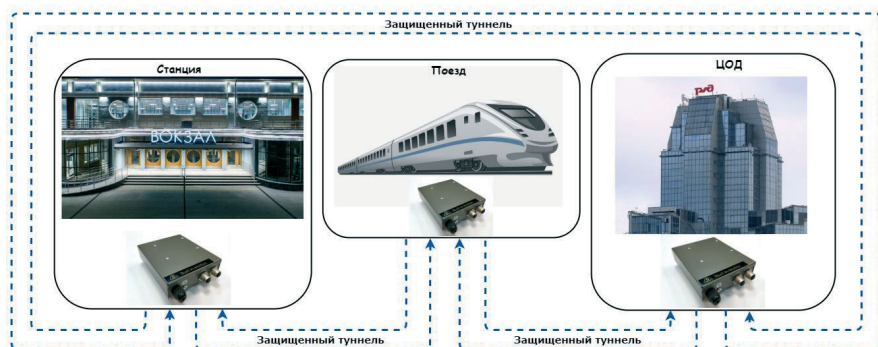


Рисунок 21 - Применение TrusT-in-Motion в инфраструктуре наземного транспорта

2. Пример защищенного сетевого взаимодействия объектов банковской транспортной инфраструктуры

Стационарное оборудование, размещенное в здании банка (ЦОД), взаимодействует с оборудованием на подвижных объектах – машинах инкассаторов, которые, в свою очередь, взаимодействуют с оборудованием банка.

Ниже на рисунке изображена организация защищенного сетевого взаимодействия объектов банковской транспортной инфраструктуры с помощью маршрутизатора TrusT-in-Motion.

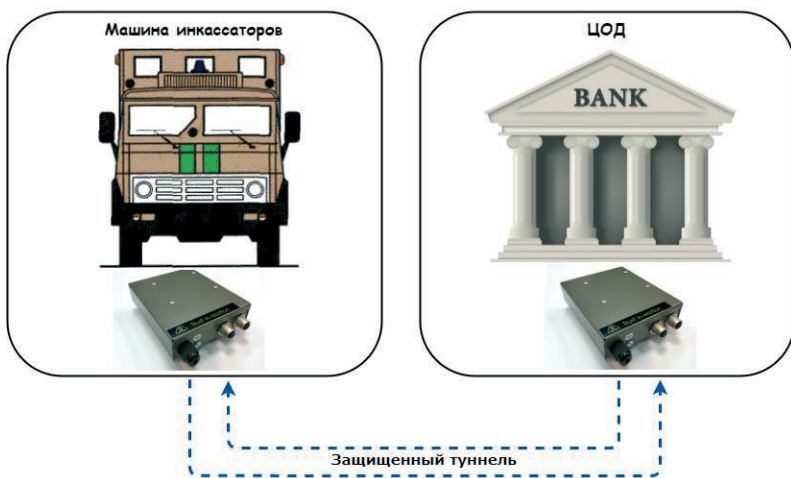


Рисунок 22 - Применение TruT-in-Motion в банковской инфраструктуре

3. Пример защищенного сетевого взаимодействия объектов инфраструктуры медицинских учреждений

Стационарное оборудование, размещенное в здании больницы, взаимодействует с оборудованием на подвижных объектах – машинах скорой помощи, которые, в свою очередь, взаимодействуют с оборудованием больниц.

Ниже на рисунке изображена организация защищенного сетевого взаимодействия объектов инфраструктуры медицинских учреждений с помощью маршрутизатора TruT-in-Motion.

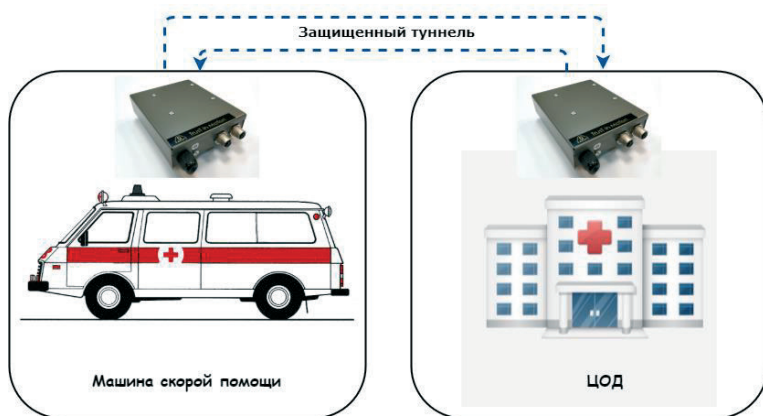


Рисунок 23 - Применение TruT-in-Motion в инфраструктуре медучреждений

4. Пример защищенного сетевого взаимодействия объектов инфраструктуры авиационного транспорта

Стационарное оборудование, размещенное в вычислительном центре (ВЦ), взаимодействует с оборудованием на подвижных объектах – самолетах, которые, в свою очередь, взаимодействуют с оборудованием ВЦ.

Ниже на рисунке изображена организация защищенного сетевого взаимодействия объектов инфраструктуры авиационного транспорта с помощью маршрутизатора TrusT-in-Motion.

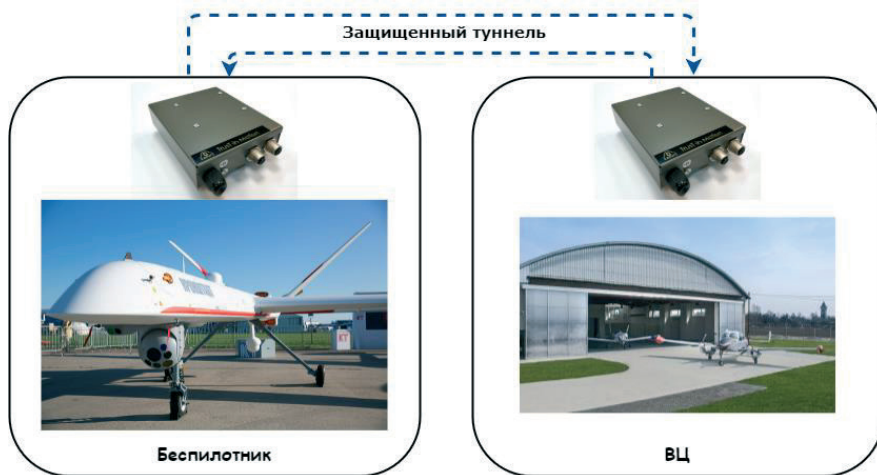


Рисунок 24 - Применение TrusT-in-Motion в инфраструктуре авиационного транспорта

4.2 СРЕДСТВА КОНТРОЛЯ ТОЧЕК ПОДКЛЮЧЕНИЯ СТОРОННИХ ОРГАНИЗАЦИЙ

Повлиять на то, как организуют информационную защиту сами подрядчики, почти невозможно (такие случаи известны, но воспользоваться этим опытом может мало какая организация). Чтобы защитить собственную информационную систему от атак, осуществляемых через взлом подрядных организаций, необходимо обеспечить собственную информационную безопасность. Для этого, как правило, нужно следовать следующим правилам:

- использовать в системе качественное антивирусное ПО;
- регулярно проводить аудит безопасности;
- контролировать точки подключения подрядных организаций.

И если первые два пункта из списка организационные, и их выполнение возлагается «на плечи» эксплуатирующей организации (выбор подходящего антивируса и разработка политики аудита безопасности, как правило, осуществляется ответственным персоналом в соответствии с внутренними регламентами), то последнее правило обязывает применять специальные средства контроля за подключениями внешних информационных системам.

К средствам мониторинга сетевых подключений относится разработанное компанией ОКБ САПР решение МЭ-TruST.

Особенностями межсетевого экрана МЭ-TruST является ощутимо более низкая стоимость, чем у аналогичных устройств на других аппаратных платформах, что обеспечивается защищенной архитектурой устройства, благодаря которой требуется ощутимо меньше наложенных средства защиты. Более подробно о МЭ-TruST рассказывается в п.п. 4.2.1.

4.2.1 МЭ-TruST

МЭ-TruST – это межсетевой экран, реализованный на базе специализированного компьютера m-TruST, обеспечивающий контроль и защиту сетевого трафика предприятия¹⁾.

МЭ-TruST позволяет эффективно решать задачи по обеспечению сетевой защиты, поддерживая работу одновременно и в режиме фильтрации сетевого трафика на уровне L2, и в режиме коммутатора и на уровне L3 в режиме маршрутизатора.

Схема работы МЭ-TruST представлена на рисунке 25:

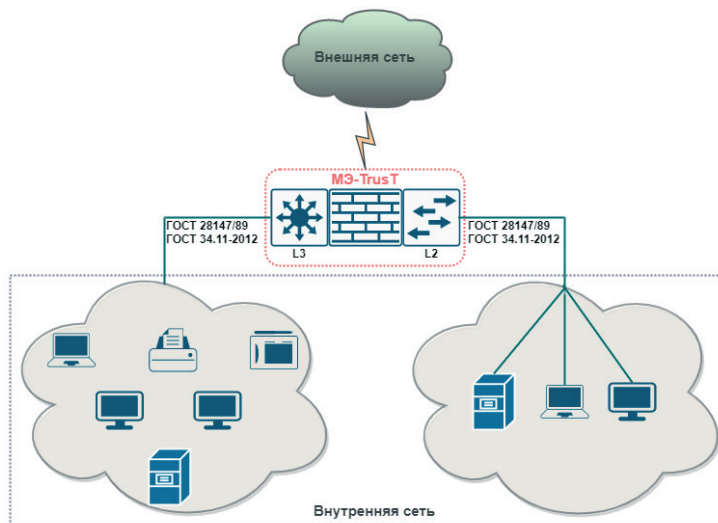


Рисунок 25 – Схема работы МЭ-TruST

¹⁾ МЭ-TruST (<https://www.okbsapr.ru/products/newharvard/METruST/>).

Помимо поддержки фильтрации трафика, к которой относятся возможность фильтрации сетевого трафика по основным полям сетевого пакета, а также по доменным именам, по расписанию, МЭ-TruST обеспечивает защиту информации от утечки, а также обнаружение и предотвращение проникновения вирусного ПО в локальную сеть.

Защита сетевого контура обеспечивается за счет наличия шифрования каналов связи с применением отечественных криптографических алгоритмов (ГОСТ 28147/89, ГОСТ 34.11-2012).

Гибкая архитектура обеспечивает «вирусный иммунитет» и позволяет эффективно реализовывать любые политики безопасности.

Достоинством МЭ-TruST является поддержка централизованного управления всех подчиненных программно-аппаратных комплексов с единого устройства.

Комплекс поддерживает прозрачную работу пользователей и других устройств, в частности, за счет наличия возможности синхронизации правил фильтрации с другими устройствами, и агрегации правил фильтрации в группы.

Межсетевой экран на базе микрокомпьютера m-TruST обеспечивает безопасное и надежное соединение между филиалами предприятия или дата-центрами. Возможность подключения большого количества удаленных внешних пользователей к внутренней сети предоставляет прозрачный доступ к ресурсам организации и защиту от внешних угроз. Высокая скорость шифрования (до 20 Гбит/с) обеспечивает быстрое подключение устройств без дополнительных требований к инфраструктуре передачи данных.

Дополнительно МЭ-TruST поддерживает возможность ведения журнала, в котором отображаются созданные правила фильтрации.

4.3 СРЕДСТВА КОНТРОЛЯ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Как правило, атаки на инфраструктуру относятся к типу целевых атак, так как при их проведении злоумышленниками преследуется какая-то конкретная цель – кража денежных средств, корпоративной информации (номера банковских счетов, договоры и декларации, персональные данные, чертежи ядерных ракет, план объектов госсектора и т.д.), нанесение ущерба работоспособности информационной системе, модификация ресурсов и т.д.

Ранее было отмечено, что к основным причинам атак на инфраструктуру можно отнести следующее:

– усложнение инструментария злоумышленников – за последнее время инструменты злоумышленников стали более интеллектуальными и сложными в детектировании, об этом свидетельствует рост¹⁾ числа атак с применением вредоносного ПО, атак через веб-приложения, атак, нацеленных на компрометацию внутренних учётных записей, ddos-атак. Помимо этого, прослеживается усложнение методов проведения атак – Supply-chain²⁾ этому доказательство: минув этап поиска уязвимостей в ИС, злоумышленники завладевают правами администратора, таким образом, перехватывая управление всей ИС;

¹⁾ Отчет Solar JSOC Security Report. Итоги года (https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf).

– бесконтрольная деятельность пользователей – несанкционированные действия в отношении инфраструктуры могут совершить непосредственные сотрудники, работающие в периметре контролируемой зоны компании, и, тем самым, поспособствовать кибератаке.

Возможные последствия:

- утечка данных;
- компрометация личных данных или учетных записей;
- заражение ИС вредоносным ПО;
- получение доступа к критичной информации;
- потеря денежных средств;
- остановка функционирования ИС.

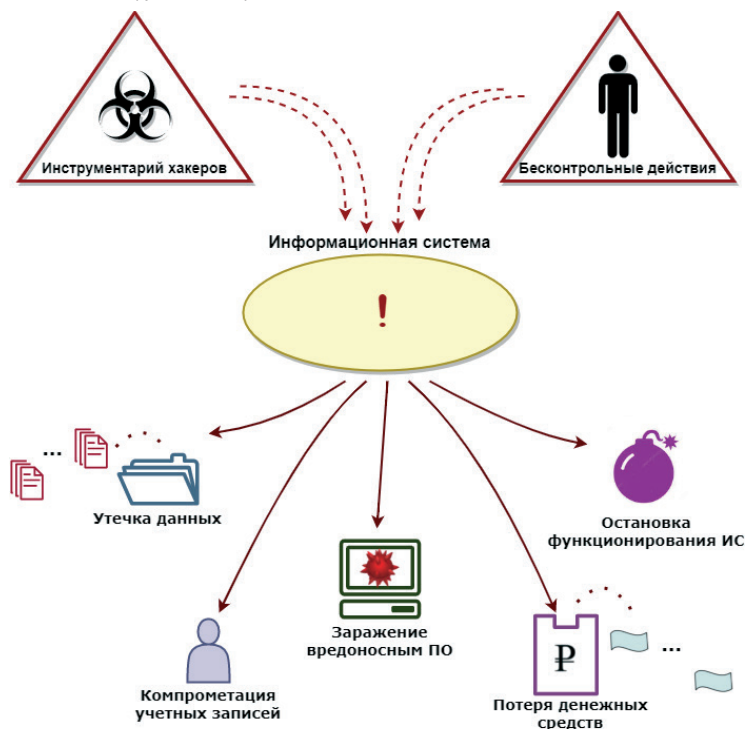


Рисунок 26 - Атаки на инфраструктуру. Причины и последствия

Чтобы предотвратить проникновение в инфраструктуру необходимо:

- обеспечить доверенную вычислительную среду и контролировать ее целостность;
- обеспечить разграничение доступа пользователей;
- контролировать работу пользователей и установленного на компьютерах ПО;
- централизованно управлять настройками;
- осуществлять мониторинг событий безопасности;
- управлять встроенными механизмами безопасности.

С целью контроля и защиты информационной инфраструктуры ОКБ САПР разработала несколько категорий продуктов, которые обладают развитой функциональностью и оказывают многостороннюю защиту ИС.

К таким категориям решений относятся:

- средства защиты от вредоносного инструментария:
 - средства доверенной загрузки:
 - ✓ средство защиты от несанкционированного доступа (СЗИ от НСД) «Аккорд-АМДЗ»;
 - ✓ СЗИ от НСД «ИНАФ»;
 - ✓ средство доверенной загрузки (СДЗ) «Аккорд-МКТ»;
 - средства защиты систем виртуализации (специальное программное обеспечение (СПО) «Аккорд-KVM», СПО «Аккорд-В.», СПО «Сегмент-В.»);
 - защищённые микрокомпьютеры m-Trust;
 - средства разграничения доступа (программно-аппаратный комплекс «Аккорд-Х», СПО «Аккорд-Win64 К», СПО «Аккорд-Х К»);
- средства контроля за работой пользователей:
 - средства централизованного управления:
 - ✓ ПАК «Центр-Т»;
 - ✓ автоматизированное рабочее место (АРМ) защищенного хранения и сетевой загрузки на базе микрокомпьютера «m-Trust»;
 - ✓ система удалённого централизованного управления «Аккорд» («СУЦУ»);
 - ✓ программный продукт (ПП) «Паспорт ПО»;
 - защищённые носители информации:
 - ✓ семейство защищенных съемных носителей: ПАК «Секрет Особого Назначения», ПАК «Секрет Фирмы», ПАК «Секрет Администратора»;
 - ✓ носители ключевой информации (ПАК «Идеальный токен»);
 - ✓ средства архивирования журналов (ПАК «ПАЖ»);
 - ✓ отчуждаемый шлюз (ПАК «Система Ниппель»);
- специальные инструменты для управления встроенными механизмами безопасности:

- USB Guard. Функциональный модуль UEFI.

Для более наглядного представления все средства контроля инфраструктуры и их виды можно представить графически:



Рисунок 27 - Средства контроля и защиты инфраструктуры ОКБ САПР

4.3.1 Средства защиты от вредоносного инструментария

Ранее в п.п. 2.3 отмечалось, что защита от вредоносного инструментария достигается за счёт:

- обеспечения доверенной вычислительной среды как в физических инфраструктурах, так и в виртуальных;
- блокировки уязвимостей используемых приложений и средств вычислительной техники (СВТ);
- контроля неизменности вычислительной среды;
- разграничения доступа к ресурсам системы.

Принципиальное отличие средств защиты от вредоносных инструментов компании ОКБ САПР заключается в наличии в них аппаратного независимого контролирующего устройства, начинающего работу до старта операционной системы ОС. Данное устройство называется резидентным компонентом безопасности (РКБ). РКБ встроен в вычислительную систему объекта и способен контролировать целостность среды путем сравнения ее параметров с эталонными.

Рассмотрим схему проведения хакерской атаки и способы блокировки этапов ее проведения.

Чтобы защититься от вредоносного инструментария, при старте работы вычислительных средств необходимо убедиться в том, что они все еще не стали инструментом злоумышленника, а затем – разграничивать доступ внутри ОС, обязательно включая контроль запуска задач.

Это не волюнтаристское утверждение, а детерминированный вывод, вытекающий из того, почему вообще компьютер может стать инструментом злоумышленника, а не легального пользователя. Такая возможность существует потому, что все современные компьютеры представляют собой реализацию концепта машины Тьюринга, универсального исполнителя, и поэтому наследуют ее архитектурную уязвимость: машина, которая создана для того, чтобы выполнять *любую* задачу, выполнит и вредоносную.

На использовании этой уязвимости основаны практически все современные хакерские атаки, которые, в основном, сводятся к атаке на «перехват управления». Схема атаки обычно выглядит так (рисунки 28):

- s1) внедряется и размещается в оперативной памяти вредоносное ПО (ВрПО);
- s2) внедряется и размещается в оперативной памяти вредоносный обработчик прерываний;
- s3) записывается в долговременную память ВрПО и обработчик прерываний;
- s4) с помощью любого доступного механизма вызывается прерывание – например, с помощью DDOS-атаки;
- s5) внедренный ранее обработчик прерываний срабатывает, и передает управление ВрПО;
- s6) ВрПО выполняет свою функцию, например, реализует разрушающее программное воздействие (РПВ).

Здесь s1 – s3 – это шаги (steps) по подготовке атаки, s4 – инициирование атаки, s5 и s6 – собственно использование архитектурной уязвимости.

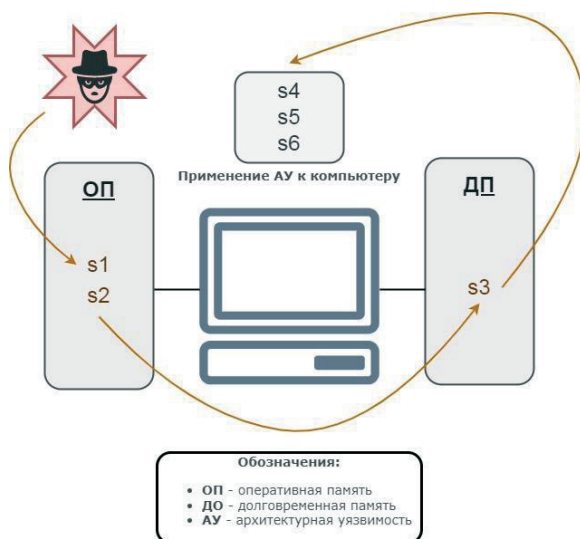


Рисунок 28 - Схема проведения атаки на перехват управления

Для того чтобы обезвредить шаги s1 и s2, обычно используются антивирусные программы. Иногда это бывает полезным, но только *иногда*, потому что невозможно с помощью антивирусных программ выявить все ВрПО. Более того – специалистам известны конструкции ВрПО, которые точно нельзя обнаружить. Можно даже сказать, что компьютерные вирусы и в целом ВрПО удастся обнаружить только в силу их несовершенства. В общем случае всегда можно разработать такое ВрПО, которое не может быть обнаружено с помощью антивирусных программ сигнатурного поиска, эвристических анализаторов и поведенческих блокираторов.

Блокирование последствий выполнения шага s3 выполняется при последующей загрузке с помощью механизмов контроля целостности – по сути, ревизоров, определяющих, есть ли изменения в составе данных; иногда эта проверка выполняется с помощью тех же наборов антивирусных программ – но это слабое решение, так как проверка должна выполняться до загрузки ОС, а программы, в том числе и антивирусные, работают под управлением ОС.

Генерация события на шаге s4 частично блокируется с помощью специальных средств анализа трафика, устанавливаемых как в сети, так и на клиентских компьютерах. Важно то, что пока нет средств, позволяющих гарантированно блокировать эту уязвимость.

Негативные последствия шагов s5 и s6 блокируются с помощью механизмов контроля запуска задач (процессов, потоков). Это очень эффективные механизмы, но реализующие их средства довольно дорогие и для их настройки нужно быть специалистом в компьютерных технологиях и информационной безопасности.

Обращает на себя внимание то, что некоторые из перечисленных функций безопасности должны выполняться до загрузки операционной системы.

Архитектурную уязвимость возможно исправить только на архитектурном уровне, а это означает:

- 1) Добавить в архитектуру компьютера (или системы) контролирующий компонент, который на время старта будет лишать систему универсальности.
- 2) Построить архитектуру, сразу лишенную этой уязвимости – такую, компьютер которой на этапе загрузки не будет являться машиной Тьюринга.

Соответственно, рассмотрим наложенные средства контроля старта систем (п.п. 4.3.1.1, 4.3.1.2), построенных на компьютерах традиционных архитектур; затем – Новую гарвардскую архитектуру: архитектуру, в которой нет уязвимости машины Тьюринга (п.п. 4.3.1.3); и затем – средства разграничения доступа, включающие контроль запуска задач (4.3.1.4).

4.3.1.1 Средства доверенной загрузки

Средства доверенной загрузки обеспечивают доверенную загрузку СВТ и его компонентов. При установке в СВТ пользователей блокируют архитектурные уязвимости СВТ, контролируют целостность объектов ИС и их настроек, обеспечивают работу пользователей в доверенной контролируемой среде.

«АККОРД-АМДЗ»

Средство доверенной загрузки уровня платы расширения – СЗИ НСД «Аккорд-АМДЗ»¹⁾ – представляет собой аппаратный модуль доверенной загрузки для IBM-совместимых ПК серверов и рабочих станций локальной сети, обеспечивающий защиту устройств и информационных ресурсов от несанкционированного доступа. Комплекс начинает работу сразу после выполнения кода системного BIOS компьютера – до загрузки операционной системы.

ПАК СЗИ НСД «Аккорд» создает доверенную среду для работы программных средств, обеспечивающих защиту компьютера на шагах s1 – s6 (см. схему проведения атаки, описанную в п.п. 4.3.1):

¹⁾ Аккорд-АМДЗ (<https://www.okbsapr.ru/products/accord/accord-amdz/>).

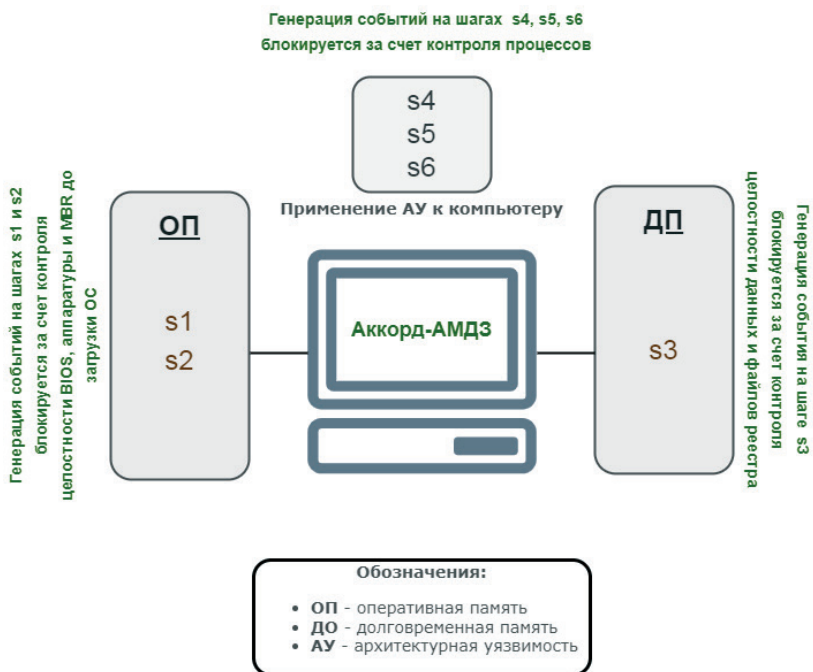


Рисунок 29 - Блокировка проведения атаки посредством «Аккорд-АМДЗ» (шаги s1-s6)

Комплекс «Аккорд-АМДЗ» реализует концепцию резидентного компонента безопасности (РКБ) – автономного примитивного перенастраиваемого устройства с защищенной памятью, способного изменить архитектуру компьютера на время старта, сделав тем самым старт защищенным.

Комплекс СЗИ НСД «Аккорд-АМДЗ» включает:

- специализированный контроллер с предустановленной на этапе изготовления резидентной операционной средой;
- функциональное программное обеспечение (ФПО), работающее в резидентной операционной среде.

Резидентная операционная среда и ФПО на этапе изготовления комплекса объединяются в единое резидентное ПО (firmware) и размещаются в энергонезависимой флэш-памяти специализированного контроллера.

Модификация контроллера определяется размером и шинным интерфейсом. Резидентная операционная среда контроллера включает:

- резидентные драйверы специализированных контроллеров;
- резидентные драйверы персональных идентификаторов.

ФПО является ядром защиты и реализует комплекс мер по защите информации от НСД.

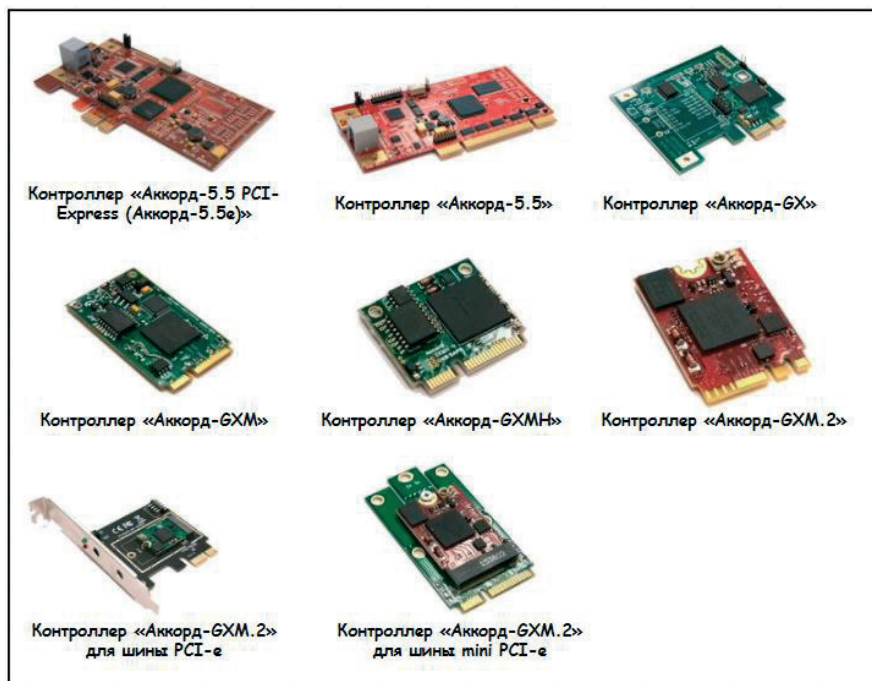


Рисунок 30 – Типы контроллеров «Аккорд-АМД3»

ПАК СЗИ НСД «Аккорд-АМД3» обеспечивает нейтрализацию следующих основных угроз безопасности информации:

- несанкционированный доступ к информации за счет загрузки нештатной операционной системы (ОС) и обхода правил разграничения доступа штатной ОС и (или) других средств защиты информации, работающих в среде штатной ОС;
- нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов аппаратного обеспечения средств вычислительной техники в информационной системе;
- нарушение целостности программного обеспечения средства доверенной загрузки;
- несанкционированное изменение конфигурации (параметров) средств доверенной загрузки;
- преодоление или обход функций безопасности средств доверенной загрузки.

«Аккорд-АМД3» обеспечивает:

- защиту ресурсов СВТ от лиц, не допущенных к работе на ней, на основе идентификации пользователей СВТ по персональным идентификаторам до загрузки ОС;

- аутентификацию пользователей с защитой от раскрытия пароля – до загрузки ОС;
- блокировку загрузки с отчуждаемых носителей (FDD, CD/DVD-ROM, ZIP, USB-накопителей и др.);
- контроль целостности технических, программных средств, условно постоянной информации СБТ до загрузки ОС, с реализацией пошагового алгоритма контроля;
- контроль целостности объектов файловых систем, размещенных на динамических дисках;
- доверенную загрузку системного и прикладного ПО при одновременной установке на дисках или в логических разделах диска СБТ нескольких ОС;
- регистрацию на СБТ пользователей;
- регистрацию контролируемых событий в системном журнале, размещенном в энергонезависимой памяти контроллера;
- возможность физической коммутации управляющих сигналов периферийных устройств, в зависимости от уровня полномочий пользователя позволяющей управлять вводом/выводом информации на отчуждаемые физические носители и устройства обработки данных;
- администрирование встроенного ПО комплекса (регистрацию пользователей и персональных идентификаторов, назначение файлов для контроля целостности, контроль аппаратной части СБТ, просмотр системного журнала);
- регистрацию, сбор, хранение и выдачу данных о событиях, происходящих в СБТ в части системы защиты от несанкционированного доступа.

СЗИ от НСД «ИНАФ»

Средство доверенной загрузки уровня платы расширения – СЗИ НСД «Инаф» представляет собой аппаратный модуль для шины USB, предназначенный для применения на автономных ПК, серверах и рабочих станциях локальной сети¹⁾.



Рисунок 31 – СЗИ НСД «ИНАФ»

СЗИ НСД «Инаф» обеспечивает выполнение следующих основных функций:

¹⁾ СЗИ НСД «Инаф» (<https://www.okbsapr.ru/products/accord/szi-nsd-inaf/>).

- аппаратный контроль целостности технических, программных средств, условно-постоянной информации СБТ до загрузки ОС, с реализацией пошагового алгоритма контроля;

- возможность доверенной загрузки операционной системы, а также системного и прикладного ПО при одновременной установке на дисках или в логических разделах диска СБТ нескольких ОС;

- автоматическое ведение протокола регистрируемых событий на этапе доверенной загрузки операционной системы (в системном журнале, размещенном в энергонезависимой памяти аппаратной части комплекса);

- администрирование встроенного ПО комплекса (генерацию пароля администратора и определение его параметров; назначение файлов для контроля целостности и режимов контроля, работу с журналом регистрации системных событий, контроль аппаратной части СБТ) и разделение прав администратора безопасности информации комплекса и пользователя СБТ;

- регистрация, сбор, хранение и выдача данных о событиях, происходящих в СБТ (РС) в части системы защиты от несанкционированного доступа.

В зависимости от конструктивных возможностей СБТ возможна как установка контроллера «Инаф» внутри корпуса СБТ в качестве штатного устройства с USB-разъемом типа А, так и подключение к штырьковому разъему непосредственно на материнской плате СБТ.

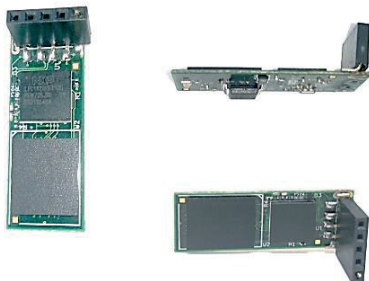


Рисунок 32 – «ИНАФ» для подключения к штырьковому разъему материнской платы

Поскольку контроллер «Инаф» реализован в форм-факторе USB-устройства, он не требует для своей установки наличия на СБТ свободного PCI-слота и может применяться в случаях, когда используются blade-серверы, в которых отсутствуют PCI-слоты, но имеются свободные внутренние или внешние USB-разъемы.

«Инаф» может использоваться в рамках реализации двух типов сценариев:

Стационарная установка в СБТ.

Данный тип сценария используется в том случае, когда необходима непрерывная реализация функционала «Инаф». В этом случае контроллер соответствующим образом настроен и подключен к USB-порту СБТ постоянно. Каждый раз перед загрузкой ОС пользователем СБТ контроллер «Инаф» выполняет процедуру контроля целостности

определенных заранее объектов. В случае нарушения целостности загрузка ОС блокируется и требуется вмешательство администратора безопасности информации (пользователя «Инаф»).

Для корректного осуществления работы по данному типу сценария необходимо:

- установить в BIOS вариант загрузки с «Инаф» как с жесткого диска;
- установить пароль на вход в BIOS;
- принять административные меры, исключающие несанкционированное отключение устройства от USB-порта:
 - ограничить физический доступ к СБТ и/или
 - зафиксировать устройства с помощью специальных креплений и/или голографической наклейки или установить контроллер внутрь корпуса СБТ.

Использование в качестве мобильного устройства.

Данный тип сценария используется в том случае, когда нет необходимости выполнять процедуры контроля целостности объектов постоянно и запрещать для пользователей СБТ загрузку ОС в случае нарушения целостности, а нужно только выявить сам факт нарушения целостности установленных на контроль объектов.

В этом случае сначала выполняются все необходимые настройки подключенного к СБТ контроллера «Инаф», затем контроллер извлекается из СБТ и хранится в надежном месте (например, в сейфе). Пользователи СБТ работают в обычном режиме, а пользователь «Инаф» периодически подключает к СБТ свой контроллер «Инаф» с целью убедиться в неизменности состава СБТ и установленных ранее на контроль объектов.

Возможен также вариант работы с СЗИ НСД «Инаф», когда контроллер подключается к СБТ каждый раз перед началом сеанса работы и извлекается из СБТ после ее выключения.

Для корректного осуществления работы по данному типу сценария обязательно должны быть предусмотрены специальные регламенты действий пользователей, в чьи обязанности входит запуск СБТ, так как наличие «Инаф» в USB-порту должны контролировать именно они.

Следует помнить о том, что поскольку для работы с «Инаф» требуется настраивать порядок загрузки ОС в BIOS компьютера, необходимо накладывать определенные ограничения (особенно в случае стационарной установки СЗИ НСД «Инаф» в СБТ) на доступ пользователей СБТ к BIOS (путем установки пароля на BIOS), а также контролировать целостность BIOS средствами «Инаф».

МДЗ «АККОРД-МКТ»

МДЗ «Аккорд-МКТ»¹⁾ является программным продуктом (специальным программным обеспечением, СПО), предназначенным для встраивания в базовую систему ввода-вывода (БСВВ) микрокомпьютеров и ЭВМ на базе процессоров с архитектурой x86_64 (далее по тексту – микрокомпьютер либо МКТ) и обеспечения выполнения основных функций его защиты от НСД, в том числе настройки, контроля функционирования и управления защитными механизмами.

Встраивание (прошивка) СПО «Аккорд-МКТ» в БСВВ выполняется производителем изделия на этапе изготовления МКТ, то есть «Аккорд-МКТ» приобретает в составе микрокомпьютера.

МДЗ «Аккорд-МКТ» обеспечивает:

МДЗ «Аккорд-МКТ» обеспечивает:

- идентификацию и аутентификацию пользователей при входе в систему по уникальному идентификатору пользователя и по паролю временного действия длиной от 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;

- идентификацию и аутентификацию пользователей при допуске к средствам настройки и администрирования МДЗ «Аккорд-МКТ» по уникальному идентификатору пользователя и по паролю 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;

- контроль целостности отдельных файлов и программных средств МКТ;

- администрирование, включающее:

- регистрацию пользователей и их идентификаторов;
- построение списков объектов для контроля целостности и указание режимов контроля;
- работу с журналом регистрации системных событий и действий пользователей.
- возможность резервного копирования на отчуждаемый носитель и восстановления базы данных пользователей и списка контролируемых объектов;

- регистрацию и учет системных событий и действий пользователей;

- защиту от вредоносного кода.

Пользователь МДЗ «Аккорд-МКТ», как и пользователи других СДЗ не столько применяет это средство защиты, сколько работает под его контролем. Взаимодействие пользователя с «Аккорд-МКТ» сводится к идентификации, аутентификации и смене пароля (по истечении срока действия или в произвольный момент времени). Остальные контрольные процедуры проводятся МДЗ самостоятельно.

Принцип работы «Аккорд-МКТ»:

¹⁾ Аккорд-МКТ (<https://www.okbsapr.ru/products/accord/accord-mkt/>).

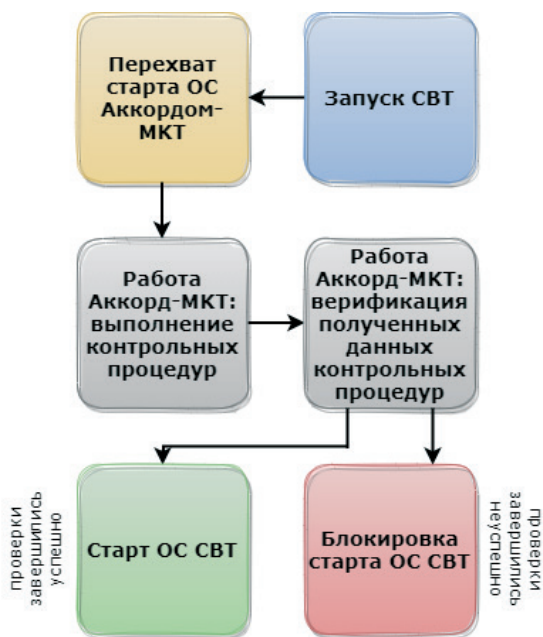


Рисунок 33 – Основной принцип работы «Аккорд-МКТ»

Контрольные процедуры делятся на обязательные, которые по умолчанию выполняются при каждом запуске микрокомпьютера, и необязательные, которые устанавливаются администратором БИ.

К обязательным процедурам контроля относятся:

- процедура идентификации оператора (пользователя);
- процедура аутентификации (подтверждение достоверности) оператора (пользователя);
- проверка целостности отдельных файлов и программных средств МКТ.

К необязательным процедурам контроля относятся:

- процедура смены пароля, выполняемая, когда время жизни пароля превысило установленный администратором БИ интервал времени;
- проверка ограничения на время входа оператора (пользователя) в систему.

4.3.1.2 Средства защиты систем виртуализации

В виртуальных средах также, как и в физических, хранится огромное количество различного рода информации и совершается множество вычислений и действий. Поэтому виртуальные среды нуждаются в защите наряду с физическими.

Для защиты виртуальных сред также, как и для физических, необходимо построить доверенную вычислительную среду.

Однако инфраструктуры виртуализации имеют в плане защиты информации отличие от физических инфраструктур: процесс их загрузки разнесен в пространстве и во времени. Создание и поддержание доверенной вычислительной среды в таких системах требует применения специально предназначенных для этого средств.

Компания «ОКБ САПР» располагает специальными средствами защиты, построенными на основе принципа непрерывности контрольных процедур: СПО «Аккорд-В.» для VMware vSphere; СПО «Аккорд-KVM» для KVM, – способными защитить инфраструктуры виртуализации.

СПО «Аккорд-KVM»

СПО «Аккорд-KVM» применяется для защиты инфраструктур виртуализации, построенных на базе KVM и использующих библиотеку libvirt в качестве инструмента управления гипервизором¹⁾.

СПО «Аккорд-KVM» включает в себя:

- модуль контроль целостности виртуальных машин;
- модуль перехвата старта виртуальных машин.

Основные защитные механизмы СПО «Аккорд-KVM» базируются на:

- контроле целостности программных компонентов ВМ (файлов общего, прикладного ПО и данных), выполняемом до их запуска;
- контроле целостности конфигурации ВМ, выполняемом до запуска ВМ;
- управлении размещением и перемещением исполняемых виртуальных машин между серверами виртуализации;
- регистрации событий безопасности в инфраструктуре виртуализации.

СПО «Аккорд-KVM» полностью интегрируется в инфраструктуру виртуализации, поэтому для его функционирования нет необходимости использовать дополнительные серверы.

СПО «Аккорд-KVM» позволяет контролировать целостность компонентов ВМ (файлов общего, прикладного ПО и данных), выполняемых до их запуска.

Общий принцип работы продукта показан на рисунке 34.

¹⁾ Аккорд-KVM (<https://www.okbsapr.ru/products/virtsys/accord-kvm/>).



Рисунок 34 - Принцип работы СПО «Аккорд-KVM»

Управляющий персонал комплекса управляет перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных, включая:

- файлы образов виртуальных машин (контейнеров) – между носителями (системами хранения данных) в целях контроля целостности конфигурации виртуальных машин;
- исполняемые виртуальные машины (контейнеры) – между серверами виртуализации с целью обеспечения возможности разрешения или запрета запуска виртуальной машины на заданном хосте;
- данные, обрабатываемые с использованием виртуальных машин, – между носителями (системами хранения данных) с целью контроля целостности конфигурации виртуальных машин.

При этом с помощью функции разрешения или запрета запуска виртуальной машины на заданном хосте можно обеспечить:

- полный запрет перемещения виртуальных машин (контейнеров);
- ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);
- ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

Также СПО «Аккорд-KVM» обеспечивает:

- возможность функционирования в демонстрационном режиме при отсутствии лицензии;
- возможность установки любого пути к файлу базы данных.

СПО «АККОРД-В.»

СПО «Аккорд-В.» предназначено для защиты инфраструктур виртуализации, построенных на базе платформы виртуализации VMware vSphere 6.7¹⁾.

СПО «Аккорд-В.» предназначено для выполнения основных функций защиты на основе:

- доверенной загрузки всех элементов ВМ инфраструктуры виртуализации;
- контроля целостности оборудования ВМ, а также BIOS и MBR ВМ, выполняемого до их запуска;
- регистрации событий о действиях в инфраструктуре виртуализации (на серверах vCenter и ESXi), а также событий агентов СПО «Аккорд-В.»;
- идентификации и аутентификации администратора безопасности при входе на ESXi сервера;
- создания и восстановления резервных копий баз данных агентов СПО «Аккорд-В.» на ESXi серверах.
- управления размещением и перемещением исполняемых виртуальных машин между контролируемыми СПО «Аккорд-В.» серверами виртуализации путем контроля запуска ВМ.



Рисунок 35 – Схема взаимодействия СПО «Аккорд-В.»

СПО «Аккорд-В.» не ограничивает в целях безопасности возможностей инфраструктуры виртуализации, оставляя доступными все ее преимущества.

Основной принцип работы:

¹⁾ Аккорд-В. (<https://www.okbsapr.ru/products/virtsys/accord-v-and-segment-v/>).

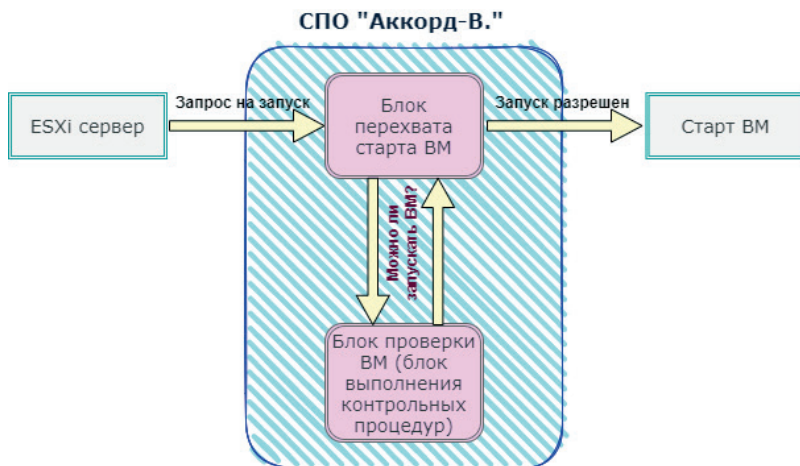


Рисунок 36 – Принцип работы СПО «Аккорд-В.»

В момент включения виртуальной машины агент СПО «Аккорд-В.», входящий в состав блока перехвата управления СПО «Аккорд-В.», осуществляет перехват старта виртуальной машины (ВМ).

После чего управление переходит блоку проверки ВМ, который, в свою очередь, проверяет разрешено ли ВМ включение на данном ESXi сервере т.е. осуществляет, таким образом, контроль миграции, а также проверку файлов BIOS, конфигурации оборудования, MBR и файлов на диске виртуальной машины (в зависимости от поставленных на контроль объектов).

По завершении проверки ВМ результат выполнения контрольных процедур возвращается в блок перехвата старта.

На основании полученного результата и принимается решение о разрешении или запрете включения ВМ.

Если ВМ разрешено включиться, то блока перехвата старта инициирует ее включение путем вызова соответствующей программы, входящей в состав СПО «Аккорд-В.».

СПО «Аккорд-В.» легко установить и настроить. Интерфейс прост в восприятии и не вызывает серьезных затруднений в работе специалистов любого уровня подготовки и квалификации. СПО «Аккорд-В.» не помешает работе других сервисов и программ, что является его несомненным преимуществом.

Недостатком СПО «Аккорд-В.» является лишь то, что данный продукт способен защитить только ВМ. Как быть, если для защиты системы потребуются обеспечить, например, доверенную загрузку ОС физического компьютера, на котором находится инфраструктура виртуализации, или же ограничить доступ пользователей к ресурсам ПК и ВМ?

На сегодняшний день, чтобы привести защиту инфраструктуры виртуализации в соответствие требованиям регуляторов (руководящие документы и приказы ФСТЭК), необходимо полагаться не на один продукт, а на совокупность решений.

Компания ОКБ САПР располагает продуктами, которые в совокупности могут обеспечить доверенную среду инфраструктуры виртуализации. К таким продуктам относится и совокупность решений «Аккорд-В».

Совокупность решений «Аккорд-В.»

Совокупность решений (СР) «Аккорд-В.» для защиты среды виртуализации – это, в первую очередь, решение, способное обеспечить доверенную вычислительную среду одновременно и в физической инфраструктуре, и в инфраструктуре виртуализации¹⁾.

СР «Аккорд-В.» – это комплексное решение, включающее в себя все необходимые элементы для реализации требований по защите информации.

СР «Аккорд-В.» дополняет продукт СПО «Аккорд-В.» в части обеспечения доверенной загрузки физической среды и разграничения доступа персонала к ресурсам «реального» СВТ и ВМ.

СР «Аккорд-В.» реализует следующие механизмы защиты:

- доверенная загрузка и контроль целостности всех элементов инфраструктуры виртуализации;
- разграничение доступа администраторов инфраструктуры виртуализации (АВИ) и администраторов безопасности информации (АБИ);
- разграничение доступа пользователей внутри виртуальных машин;
- механизмы дискреционного/мандатного контроля доступа пользователей и процессов к защищаемым объектам инфраструктуры виртуализации, включая ресурсы внутри ВМ;
- механизм очистки оперативной и внешней памяти путём записи маскирующей информации в память при её освобождении (перераспределении);
- аппаратная идентификация всех пользователей и администраторов инфраструктуры виртуализации.

¹⁾ Совокупность решений «Аккорд-В.» (<https://www.okbsapr.ru/products/virtsys/accord-v-and-segment-v/main-segment-v/>).

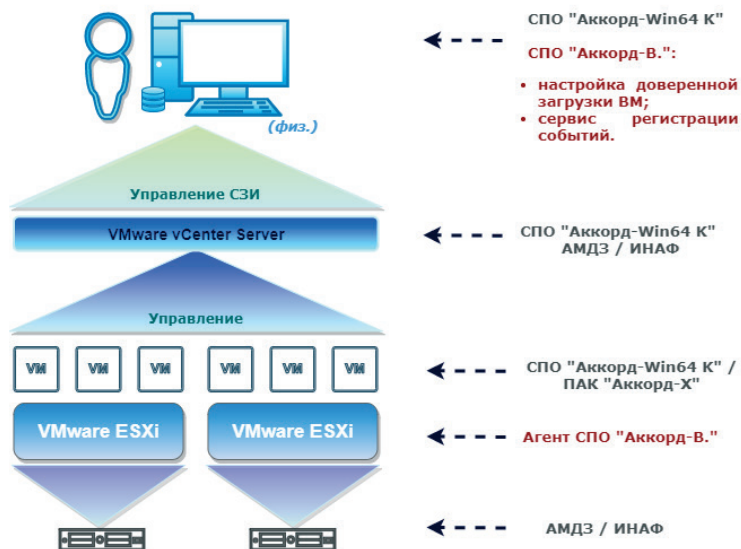


Рисунок 37 – Схема взаимодействия CP «Аккорд-B.»

Каждое из решений, входящих в состав CP «Аккорд-B.», является самостоятельным продуктом, призванным решить определенную цель. А в совокупности эти решения становятся средством, основанным на принципе непрерывности контрольных процедур и обеспечивающим контроль целостности и доверенную загрузку как физического оборудования, так и инфраструктуры виртуализации:

- на физическом уровне выполняется контроль целостности оборудования физических серверов, затем – файлов ОС;
- на виртуальном уровне – проверяются файлы BIOS и конфигурации оборудования, затем MBR и файлы ОС VM.

Данный механизм позволяет получить доверенную изолированную программную среду внутри виртуальных машин.

Попытка дискредитации хотя бы одного из «слоев» механизма контроля приводит к блокировке работы инфраструктуры виртуализации.

При проектировании системы безопасности инфраструктуры виртуализации архитектор сталкивается с рядом проблем, среди которых всегда присутствуют:

- проблема «суперпользователя» – то есть сосредоточение максимальных привилегий в рамках одной роли (пользователя). Для большинства систем такое положение неприемлемо, Администратор безопасности информации (АБИ) должен иметь возможность ограничивать действия Администратора инфраструктуры виртуализации (АВИ): запрещать критичные для безопасности действия и разрешать некоторые только по согласованию, например, удаление виртуальной машины (нарушение целостности и доступности) или экспорт ее на диск (нарушение конфиденциальности).

– проблема сегментирования – то есть разбиения системы на сегменты и обеспечения их изоляции. Так как система может содержать различную информацию (иерархически категорируемую, то есть разного уровня секретности, или неиерархически, то есть разного вида), может возникнуть ситуация, при которой она будет «перемешана». Например, случайное или умышленное переключение секретной ВМ в подсеть к несекретным или миграция ВМ разработчика на хранилище бухгалтерии.

К сожалению, данные проблемы не могут быть эффективно решены средствами самой инфраструктуры виртуализации. В итоге приходится подходить к вопросу «нестандартно», что ведет либо к дополнительным затратам, либо к снижению эффективности использования средств виртуализации, либо к введению дополнительных организационных мер усложняющих работу АБИ. По этой причине логичным шагом является перенимание опыта из смежных областей и использование наложенного средства защиты для ухода от описанных проблем.

СПО «СЕГМЕНТ-В.»

Таким средством для инфраструктур виртуализации на базе VMware vSphere (версий 5.x и 6.x, для версии 6.5 и выше поддерживается работа с HTML5 клиентом) является программно-аппаратный комплекс «Сегмент-В.»¹⁾.

ПАК «Сегмент-В.» представляет собой комплекс программных и аппаратных средств, предназначенный для разграничения доступа пользователей к объектам инфраструктуры виртуализации VMware vSphere. При этом комплекс обеспечивает защиту от утечек информации, предоставляя возможность работы под одной учетной записью с различными сегментами инфраструктуры виртуализации, запрещая их смешивание.

«Сегмент-В.» не требует установки дополнительного ПО на АРМ администраторов инфраструктуры и позволяет «бесшовно» интегрировать систему защиты в инфраструктуру виртуализации vSphere. При этом поддерживается режим Linked mode для vCenter, а также сохраняется возможность использования vCenter в качестве виртуальной машины (в том числе VCSA – VMware vCenter Server Appliance).

Основу комплекса составляет прокси-сервер, устанавливаемый в разрыв между vCenter сервером и рабочим местом администратора инфраструктуры виртуализации.

¹⁾ ПАК «Сегмент-В.» (<https://www.okbsapr.ru/products/virtsys/accord-v-and-segment-v/main-segment-v/>).

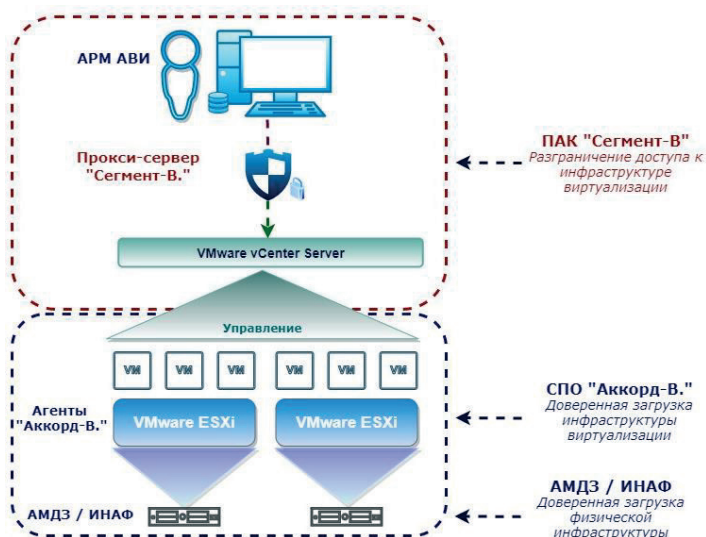


Рисунок 38 – Назначение «Сегмент-В.»

В программно-аппаратном комплексе «Сегмент-В.» реализованы следующие механизмы защиты:

- идентификация/аутентификация пользователей управляющих инфраструктурой виртуализации;
- управление миграцией виртуальных машин;
- регистрация событий в инфраструктуре виртуализации;
- разграничение доступа к объектам инфраструктуры виртуализации;
- мандатное (иерархические и неиерархические метки);
- дискреционное (более 20 действий);
- сегментирование инфраструктуры виртуализации (т.е. запрет смешивания информации из различных Сегментов). При этом система защиты:
 - работает «прозрачно» (т.е. не требуется дополнительное ПО для работы АВИ);
 - поддерживает отказоустойчивые кластерные конфигурации;
 - позволяет работать с любым вариантом инфраструктуры VMware vSphere (VCSA / Windows vCenter / Linked режим / Standalone ESXi).

Общий принцип работы:



Рисунок 39 – Принцип работы «Сегмент-В.»

При доступе администратора инфраструктуры виртуализации к сервисам vCenter и настройкам ESXi прокси-сервер, входящий в состав ПАК «Сегмент-В.», осуществляет перехват команд управления vCenter/ESXi.

При этом на основе заранее заданных правил разграничения доступа выполняется проверка разрешено ли данному пользователю получить доступ к ресурсам инфраструктуры виртуализации: выполняются процедуры идентификации и аутентификации, а также обеспечивается динамический контроль целостности исполняемых файлов из состава ПАК «Сегмент-В.».

Параллельно с этим проверяется разрешено ли ВМ включение на данном ESXi сервере, т.е. осуществляет контроль миграции виртуальной машины.

По завершении проверки принимается решение о разрешении или запрете доступа пользователя к тому или иному ресурсу инфраструктуры виртуализации.

4.3.1.3 Защищённые микрокомпьютеры «m-TruST»

В п.п. 4.3.1 было рассказано о том, что архитектурная уязвимость, присущая всем компьютерам, построенным по модели машины Тьюринга, можно блокировать только лишив его базового свойства машины Тьюринга – универсальности – на этапе загрузки.

Рассмотренные выше способы реализации этого подхода базируются на том, что нужно установить для этого в компьютер с уязвимой архитектурой (архитектурой фон-Неймана, x86).

Но в п.п. 4.3.1 также упоминалось и другое направление – создание компьютерной архитектуры, лишенной этой уязвимости.

Такая архитектура создана нами на основе Гарвардской. Гарвардской архитектуре также присуща базовая уязвимость машины Тьюринга, однако, у нее есть существенное

отличие: потоки команд и данных в ней разделены. Остается только сделать память неизменяемой, как это сделано, например, в решениях класса СОДС, о которых рассказывалось в п.п. 4.1.1.

Но пользователи ждут от компьютера универсальности, более того, возможность записи зачастую требуется программам и ОС.

Новая гарвардская архитектура – динамически изменяемая. Она построена таким образом, что включает в себя сеансовую память, доступную на запись – это дает возможность нормально работать, но сохранять эталонное состояние вычислительной среды.

СПЕЦИАЛИЗИРОВАННЫЕ МИКРОКОМПЬЮТЕРЫ «M-TRUST»

На этой архитектуре можно строить разнообразные компьютеры и микрокомпьютеры. Сегодня основной линейкой является линейка специализированных компьютеров с аппаратной защитой данных «m-TrusT», решения на основе которых уже упоминались в п.п. 4.1, 4.2.

Защищённые микрокомпьютеры «m-TrusT» представляют собой одноплатные компьютеры Новой гарвардской архитектуры, с общим назначением – защищенная сетевая коммуникация между элементами критической информационной инфраструктуры (КИИ)¹⁾.



Рисунок 40 - Общий вид микрокомпьютера m-TrusT (универсальный модуль мезонин)

Конструктивно этот компьютеры включают в себя док-станцию, которая при необходимости стационарно включается в состав элемента КИИ, и подключаемого к ней

¹⁾ Новая Гарвардская архитектура (<https://www.okbsapr.ru/products/newharvard/>).

универсального по своему аппаратному исполнению модуля – мезонина (m в названии микрокомпьютера – это именно «мезонин»).

Док-станция предназначена для того, чтобы корректно подключить «m-TrusT» к тому или иному конкретному элементу КИИ, поэтому ее конструктивное решение и набор портов могут существенно различаться, ведь такими элементами могут быть самые разные объекты – от локомотивов до банкоматов, от газовых счетчиков до терминалов управления АЭС.

Ресурсы «m-TrusT» позволяют обеспечить среду функционирования криптографии, позволяющую сертифицировать вариант исполнения СКЗИ на «m-TrusT» на класс КСЗ (такие СКЗИ есть – это, например, решения ССВТ УД «TrusT Удалёнка» (п.п. 4.1.2), защищённые терминалы «m-TrusT Терминал» и «Центр-TrusT» (п.п. 4.1.4), криптошлюзы fin-TrusT (п.п. 4.1.5), каналный шифратор «TrusT-in-Motion» (п.п. 4.1.6)). Помимо Новой гарвардской архитектуры защищённость платформы обеспечивается РКБ, встроенным в основной аппаратный блок компьютера, и СДЗ, сертифицированным ФСТЭК России.

В зависимости от того, какие элементы КИИ должны взаимодействовать (подвижной состав и станционное оборудование, банкомат и АБС, какое-то измерительное оборудование и центр обработки (или центры агрегации) данных измерений, и т. д.) – ПО активной части «m-TrusT», «мезонина» – будет разным. Оно создается для каждой конкретной задачи, поэтому Заказчиком приобретается не прибор, а решение, компонент именно той КИИ, для которой создается конкретная партия «m-TrusT».

Функциональное программное обеспечение защищено вирусным иммунитетом Новой гарвардской архитектуры – оно загружается из памяти резидентного компонента безопасности (РКБ), которая защищена от вирусного заражения.

Съемный конструктив «мезонина» неосцимемо упрощает обслуживание системы и ускоряет восстановление работоспособности при выходе «мезонина» из строя (что имеет огромное значение для КИИ) – он просто заменяется на новый путем подключения этого нового экземпляра к той же самой док-станции. Поскольку такой АРМ не хранит практически никаких данных, замена его рабочей части для системы не ощутима, если заранее сформирован некоторый фонд запасных устройств, обеспеченных нужными ключами и настройками.

При этом «m-TrusT» обеспечивает существенные преимущества, в том числе:

- работа в автоматическом режиме, что существенно снижает нагрузку на организационно-технические меры при эксплуатации СКЗИ;
- изменение форм-фактора без повторной сертификации изделия, что значительно сокращает сроки работ по защите КИИ;
- обеспечивается работа с любыми каналами связи, используемыми в КИИ;
- обеспечивается защита КИИ без глубокой переработки ее структуры, что сильно сокращает затраты на проведение мероприятий.

4.3.1.4 Средства разграничения доступа

Средства разграничения доступа позволяют разграничить доступ пользователей к корпоративным ресурсам различных категорий доступа в соответствии с их уровнями доступа в различных ОС (Windows, Linux) и средах виртуализации (VMware vSphere).

В средствах разграничения доступа ОКБ САПР имеется возможность ограничения доступа пользователей двумя методами: дискреционный и мандатный.

Программное обеспечение этих средств позволяет администратору безопасности информации реализовать правила разграничения доступа на основе набора атрибутов:

Операции с файлами

R - разрешение на открытие файлов только для чтения

W - разрешение на открытие файлов для записи

C - разрешение на создание файлов на диске

D - разрешение на удаление файлов

N - разрешение на переименование файлов

V - видимость файлов

O - эмуляция разрешения на запись информации в открытый файл

Операции с каталогами

M - создание каталогов на диске

E - удаление каталогов на диске

G - разрешение перехода в этот каталог

n - переименование подкаталогов

S - наследование прав на все вложенные подкаталоги

1 - наследование прав на 1 уровень вложенности

0 - запрет наследования прав на все вложенные подкаталоги

Прочее

X - разрешение на запуск программ

Регистрация

г - регистрация в журнале операций чтения при обращении к объекту

w - регистрация в журнале операций записи при обращении к объекту

меток доступа, которые могут быть поименованы как уровни секретности либо другим, более удобным образом (количество меток допуска может достигать шестнадцати);

и параметров:

– перечень файлов, целостность которых должна контролироваться системой, и опции контроля;

– запуск стартовой задачи (для функционально замкнутых систем);

– наличие, либо отсутствие привилегий супервизора;

– детальность журнала доступа;

– назначение/изменение пароля для аутентификации;

– временные ограничения - время по дням недели (с дискретностью 30 мин), в которое разрешено начало работ для данного субъекта;

– параметры управления экраном - гашение экрана через заранее определенный интервал времени (в случае, если в течение указанного интервала действия оператором не выполнялись), подача соответствующих звуковых и визуальных сигналов.

ПАК «АККОРД-Х»

Функции доверенной загрузки СВТ с возможностями разграничения доступа совмещает ПАК «Аккорд-Х»¹⁾.

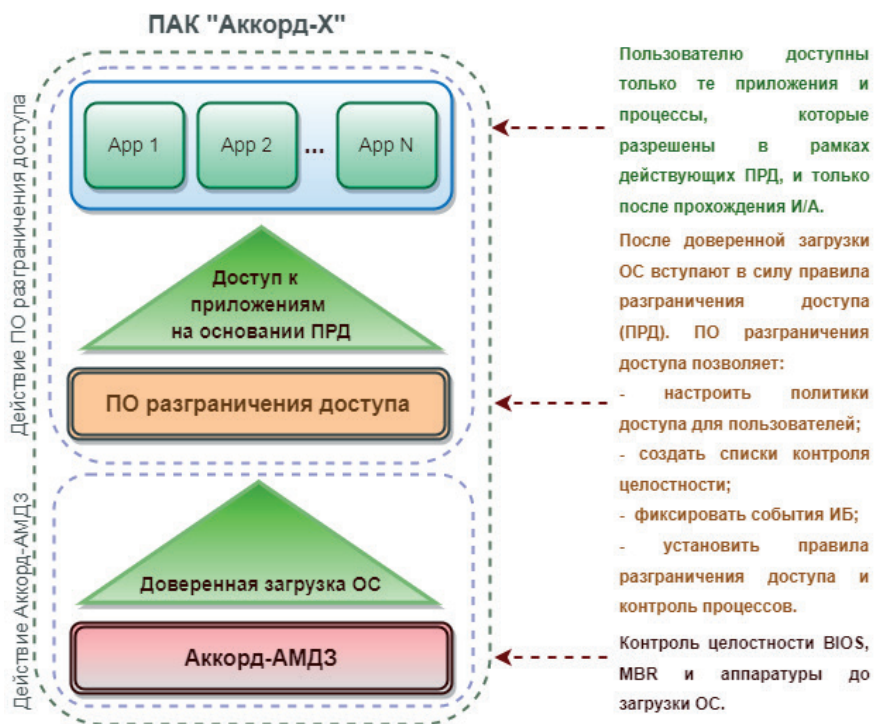


Рисунок 41 - Принцип работы ПАК «Аккорд-Х»

ПАК «Аккорд-Х» предназначен для разграничения доступа пользователей к СВТ под управлением ОС семейства Linux.

ПАК «Аккорд-Х» обеспечивает:

– защиту от несанкционированного доступа к СВТ (включая возможность ограничения разрешенных часов работы каждого пользователя);

¹⁾ ПАК СЗИ НСД «Аккорд-Х» (<https://www.okbsapr.ru/products/accord/pak-szi-nsd-accord-x/>).

- идентификацию/ аутентификацию пользователей до загрузки операционной системы с возможностью последующей передачи результатов успешной идентификации/аутентификации в ОС;
- аппаратный контроль целостности системных файлов;
- доверенную загрузку ОС;
- статический и динамический контроль целостности данных, их защита от несанкционированных модификаций;
- разграничение доступа пользователей, процессов, к массивам данных (объектам) с помощью дискреционного контроля доступа;
- разграничение доступа пользователей, процессов, к массивам данных (объектам) с помощью мандатного контроля доступа;
- разграничение доступа пользователей к определенным процессам.
- контроль доступа к периферийным устройствам.
- создание индивидуальной для каждого пользователя изолированной рабочей программной среды;
- автоматическое ведение протокола регистрируемых событий;
- контроль печати на локальных и сетевых принтерах, протоколирование вывода данных на печать, маркировка распечатанных данных (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация).

Наличие собственной системы разграничения доступа (мандатный и дискреционный методы контроля доступа) – действия, разрешенные прикладным ПО, но запрещенные СЗИ от НСД «Аккорд» – будут запрещены пользователю.

В течение всего сеанса работы пользователя ведется подробный журнал событий, в котором фиксируются все действия пользователя (существует возможность настраивать уровень детальности журнала).

Программное обеспечение комплекса позволяет администратору безопасности информации описать любую не противоречивую политику безопасности на основе наиболее полного набора атрибутов, меток доступа, которые могут быть поименованы как уровни секретности либо другим, более удобным образом (количество меток допуска может достигать шестнадцати); и параметров:

- перечень объектов и прав доступа к ним для конкретного субъекта;
- перечень объектов и прав доступа к ним для группы субъектов;
- перечень объектов, целостность которых должна контролироваться системой (статический и/или динамический контроль целостности), для конкретного субъекта;
- перечень объектов, целостность которых должна контролироваться системой (статический и/или динамический контроль целостности), для группы субъектов;
- перечень системных возможностей субъекта ();
- перечень системных настроек;
- уровень детальности журнала регистрации событий;
- назначение/изменение пароля для аутентификации;

- назначение/изменение идентификатора (ТМ, ПСКЗИ ШИПКА)
- временные ограничения - время по дням недели (с дискретностью 30 мин), в которое разрешено начало работ для данного субъекта;

Сильной стороной комплекса является наличие модуля контроля печати, который предоставляет возможность маркировки данных, выводимых на печать на сетевых и локальных принтерах, с протоколированием всех действий пользователя. Модуль контроля печати «Аккорд-Х» обрабатывает при печати документов из любого прикладного программного обеспечения, предусматривающего возможность вывода документа/файлов/данных на печать (не только OpenOffice и прочих текстовых редакторов). Контроль печати осуществляется на уровне подсистемы печати Linux, поэтому данные выводимые на печать из консоли также маркируются в соответствии с настройками подсистемы контроля печати «Аккорд-Х».

В качестве маркера (штампа) может выступать, например, гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация.

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ РАЗГРАНИЧЕНИЯ ДОСТУПА

На сегодняшний день компанией ОКБ САПР разработаны специальные программно-аппаратные комплексы средств защиты информации (ПАК СЗИ) «Аккорд-Win32», «Аккорд-Win64» для ОС семейства Windows и «Аккорд-Х» для ОС семейства Linux.

С их помощью можно реализовать следующие основные функции безопасности:

- доверенная загрузка компьютера;
- идентификация/аутентификация пользователя;
- контроль целостности системной области диска, системных файлов, программ и данных;
- разграничение доступа пользователей к ресурсам компьютера;
- ведение протокола регистрируемых событий.

Однако для некоторых систем доверенная загрузка компьютера не является необходимой для реализации. К таким относятся:

- системы, для которых необходима защита информационных ресурсов от несанкционированного доступа, а целостность критичных файлов операционной системы (ОС) уже достоверно подтверждена до загрузки ОС (например, с помощью СЗИ НСД «Инаф») или обеспечена технологически;
- системы, в которых для удовлетворения требований по безопасности не требуется обеспечение доверенной загрузки средств вычислительной техники.

Это государственные информационные системы, в которых обрабатывается информация минимального уровня значимости, или государственные информационные системы регионального или объектового масштаба, в которых обрабатывается информация низкого уровня значимости (в соответствии с приказом ФСТЭК № 17), а

также информационные системы персональных данных 3 и 4 уровня защищенности (в соответствии с приказом ФСТЭК № 21).

В таких случаях при применении ПАК СЗИ набор функций защиты будет избыточным. Поэтому компанией ОКБ САПР было разработано СЗИ, реализующее все функции ПАК СЗИ, кроме функции доверенной загрузки, не требуемой для указанных систем – специальное программное обеспечение «Аккорд-Win64 К» и «Аккорд-Х К» (для ОС Windows и Linux соответственно).

«Аккорд-Win64 К» включает в себя СПО для 32-х и 64-х разрядных ОС, установку того или другого пользователь выбирает при начале инсталляции. СПО предназначено для разграничения доступа к рабочим станциям, терминалам, терминальным серверам и поддерживает работу со средствами идентификации пользователя.

СПО СЗИ «Аккорд-Х К» предназначено для разграничения доступа к рабочим станциям, функционирующим под управлением ОС семейства Linux.

В состав СПО разграничения доступа входят средства разграничения доступа, которые условно можно представить в виде подсистем:



Рисунок 42 - Подсистемы СПО разграничения доступа

СПО «Аккорд-Win64 К»

СПО «Аккорд-Win64 К»¹⁾ представляет собой средство защиты информации (СЗИ), реализующее функции разграничения доступа к рабочим станциям, терминалам, терминальным серверам с ОС семейства Windows и поддерживает работу со средствами идентификации пользователя, применяется для

– систем, для которых необходима защита информационных ресурсов от несанкционированного доступа, а целостность критичных файлов операционной

¹⁾ СПО «Аккорд-Win64 К» (<https://www.okbsapr.ru/products/accord/spo-accord-win64-k/>).

системы (ОС) уже достоверно подтверждена до загрузки ОС (например, с помощью СЗИ НСД «Инаф») или обеспечена технологически;

- систем, в которых для удовлетворения требований по безопасности не требуется обеспечение доверенной загрузки средств вычислительной техники. Это государственные информационные системы, в которых обрабатывается информация минимального уровня значимости, или государственные информационные системы регионального или объектового масштаба, в которых обрабатывается информация низкого уровня значимости (в соответствии с приказом ФСТЭК № 17), а также информационные системы персональных данных 3 и 4 уровня защищенности (в соответствии с приказом ФСТЭК № 21).

«Аккорд-Win64 К» включает в себя СПО для 32-х и 64-х разрядных ОС, установку того или другого пользователь выбирает при начале инсталляции.

Возможности:

- защита от несанкционированного доступа;
- идентификация/аутентификация пользователей для входа в ОС;
- статический и динамический контроль целостности данных, их защита от несанкционированных модификаций;
- создание индивидуальной для каждого пользователя изолированной программной среды;
- запрет запуска неразрешенных программ;
- разграничение доступа пользователей к массивам данных и программам с помощью дискреционного контроля доступа;
- разграничение доступа пользователей и процессов к массивам данных с помощью мандатного контроля доступа;
- автоматическое ведение протокола регистрируемых событий;
- управление терминальными сессиями;
- контроль печати на принтерах, подключенных как к терминальным серверам, так и к пользовательским терминалам.
- контроль доступа к USB-устройствам.

СПО «Аккорд-Win64 К»:

- позволяет установить временной интервал, в который загрузка СБТ запрещена;
- позволяет контролировать целостность системной области диска, системных файлов, программ и данных;
- имеет собственную систему разграничения доступа;
- поддерживает управление потоками информации;
- поддерживает механизм блокировки экрана после некоторого установленного времени неактивности, который дополнен функцией идентификации пользователя при разблокировании СБТ;
- позволяет контролировать печать из любого прикладного программного обеспечения и маркировать выводимые на печать документы (в качестве маркера может

выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация).

Возможно использование вместо пароля (или одновременно с паролем) биометрической аутентификации пользователя.

СПО «Аккорд-Х К»

Аналогично СПО «Аккорд-Win64 К» существует СЗИ для ОС Linux – это СПО «Аккорд-Х К»¹⁾ – включает в себя все функции ПАК «Аккорд-Х К», кроме доверенной загрузки функции.

СПО СЗИ Аккорд-Х К предназначено для разграничения доступа к рабочим станциям, функционирующим под управлением ОС семейства Linux.

Возможности:

- защита от несанкционированного доступа;
- идентификация/аутентификация пользователей для входа в ОС;
- статический и динамический контроль целостности данных, их защита от несанкционированных модификаций;
- создание индивидуальной для каждого пользователя изолированной программной среды;
- разграничение доступа пользователей к массивам данных и программам с помощью дискреционного контроля доступа;
- разграничение доступа пользователей и процессов к массивам данных с помощью мандатного контроля доступа;
- автоматическое ведение протокола регистрируемых событий;
- контроль печати на локальных и сетевых принтерах.

СПО СЗИ Аккорд-Х К:

- позволяет установить предельно допустимый порог неудачных попыток аутентификации;
- позволяет контролировать целостность системных файлов, программ и данных;
- имеет собственную систему разграничения доступа;
- предотвращает доступ к остаточной информации при освобождении (распределении) памяти;
- поддерживает управление потоками информации, при этом обработка информации определённого уровня конфиденциальности выполняется только с помощью выделенных программ (процессов);
- позволяет блокировать множество параллельных сессий пользователя;
- поддерживает механизм блокировки экрана после некоторого установленного времени неактивности, который дополнен функцией идентификации пользователя при разблокировании СВТ;

¹⁾ СПО «Аккорд-Х К» (<https://www.okbsapr.ru/products/accord/spo-accord-x-k/>).

– позволяет контролировать печать из любого прикладного программного обеспечения и маркировать выводимые на печать документы (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация).

«Аккорд-Х К» может поставляться в двух вариантах:

1. записанное на дистрибутивном носителе (CD или USB-накопителе) СПО Аккорд-Х К, которое устанавливается на СБТ под управлением ОС Linux, и средства идентификации пользователя.
2. Аккорд-Х К в составе средства обеспечения доверенного сеанса связи (СОДС) МАРШ! — программно-аппаратный комплекс, состоящий из СОДС «МАРШ!» с предустановленным на этапе производства специальным ПО разграничения доступа и средств идентификации пользователя.

4.3.2 Средства контроля за работой пользователей

В п.п. 2.2 говорилось о том, что контроль за работой пользователей состоит, как правило, из следующих действий:

- управление рабочими местами (удалённая установка ПО рабочих мест, управление настройками и обновлением, инвентаризация). К средствам управления рабочими местами относятся продукты ПАК «Центр-Т» и АРМ защищённого хранения и сетевой загрузки;
- проверка состава ПО на рабочих местах. Проверка состава ПО на рабочих компьютерах пользователей – это одна из основных задач решения «Паспорт ПО»;
- удалённое управление СЗИ, установленными на рабочих местах, их настройками и журналами работы пользователей. К средствам удалённого управления относится СУЦУ СЗИ НСД;
- применение защищённых съёмных носителей для хранения и переноса служебной информации. К защищённым носителям относятся: защищённые флешки «Секрет», носители ключевой информации, средства архивирования журналов, отчуждаемый шлюз.

Подробнее о данных средствах будет говориться далее, в настоящем подразделе (ПАК «Центр-Т», СУЦУ СЗИ от НСД, ПП «Паспорт ПО») и подразделе 4.3.2.2, в котором речь пойдет о защищённых съёмных носителях информации «Секрет».

Инфраструктурные решения компании ОКБ САПР практически не меняют исходную архитектуру ИС, но при этом преобразуют её в более гибкую, легко администрируемую ИС, в которой возможно централизованно управлять конфигурациями рабочих мест, просматривать состав наборов ПО, контролировать целостность настроек рабочих мест и СЗИ.

4.3.2.1 Средства централизованного управления рабочими местами и настройками СЗИ

Применение систем централизованного управления рабочими местами позволяют решить такие проблемы, как:

- инвентаризация рабочих мест;
- контроль за установкой ПО;
- контроль за обновлением ПО;
- централизованное распространение ПО;
- удаленное управление рабочими местами.

Такие системы позволяют упростить процессы администрирования информационной структуры, обеспечить гибкое и быстрое развертывание систем и последующим их сопровождением в условиях минимальных затрат.

ПАК «Центр-Т»

ПАК СЗИ НСД «Центр-Т» представляет собой комплекс программных и аппаратных средств, позволяющий осуществлять централизованную контролируемую загрузку образов ПО на клиентские рабочие станции, а также их централизованное администрирование и контроль целостности¹⁾.

В общем случае «Центр-Т» предполагает использование существующей инфраструктуры – без приобретения дополнительных СВТ. С входящих в его состав специальных носителей ПО обеспечивается развертывание как серверных компонентов комплекса, так и клиентских рабочих мест.

Защищённая сетевая загрузка образов ПО на рабочие станции (РС) производится в 2 этапа.

1) На первом с отжуждаемого носителя (специального носителя ПО «Клиент Центр-Т») загружается образ ОС, называемый образом начальной загрузки (ОНЗ). ОНЗ на отжуждаемом носителе хранится в разделе, доступном только на чтение, тем самым обеспечивается загрузка целостной и аутентифицированной ОС из аутентифицированного источника. Основное и единственное назначение ОНЗ – обеспечение защищенности второго этапа загрузки.

2) Второй этап – сетевая загрузка того программного обеспечения, посредством которого производится подключение к серверу (сервер может быть терминальным или, например, это может быть инфраструктура виртуализации с виртуальными рабочими столами или веб-сервер).

Загружаемое по сети на рабочие станции ПО рассылается с Сервера хранения и сетевой загрузки (СХСЗ). Это серверный элемент инфраструктуры «Центр-Т», ПО которого (включая ОС), в свою очередь, загружается на произвольное СВТ со специального носителя ПО СХСЗ.

¹⁾ ПАК Центр-Т (<https://www.okbsapr.ru/products/management/PAKTSENTRT/>).



Рисунок 43 – Схема решения «Центр-Т»

ПО на рабочие станции загружается с Сервера хранения и сетевой загрузки (СХСЗ). Это элемент инфраструктуры «Центр-Т», сервер, ПО которого (включая ОС) загружается на произвольное СБТ со специального носителя ПО СХСЗ.

Все компоненты «Центр-Т» размещены на специальных носителях информации, и могут исполняться, загружаясь с этих носителей, на любом ПК. Это обеспечивает комплексу значительную аппаратную независимость. После отключения носителей на ПК не остается никаких компонентов комплекса или используемых им данных.

В зависимости от того, какое именно ПО содержится на специальном носителе, различаются:

- носитель ПО СХСЗ, с него загружается сервер хранения и сетевой загрузки;
- носитель ПО «Клиент Центр-Т», с которого загружаются рабочие станции (PC);
- носитель автоматизированного рабочего места (АРМ) Эмиссии, с которого загружается, соответственно, АРМ Эмиссии.

Эти носители подключаются к СБТ, которые в инфраструктуре эксплуатирующей организации будут использоваться в качестве СХСЗ, клиентских терминалов и АРМ Эмиссии соответственно. Именно это делает возможным использовать в развертываемой инфраструктуре уже имеющиеся СБТ¹⁾.

Если же нет задачи использовать имеющиеся СБТ, все три вида аппаратных компонентов инфраструктуры «Центр-Т» можно приобрести реализованными «под ключ», на базе специализированных микрокомпьютеров с аппаратной защитой данных

¹⁾ С учетом следующих ограничений:

- архитектура процессора x86-64 с поддержкой аппаратной виртуализации;
- наличие 2 гигабайт оперативной памяти;
- возможность загрузки с USB-носителей.

«m-TruST». В таком случае СХСЗ представляет собой защищенное автоматизированное рабочее место ХСЗ (далее по тексту – защищенное АРМ ХСЗ), а клиентское рабочее место – защищенный терминал «Центр-TruST»¹⁾).

В состав программной части ПАК СЗИ НСД «Центр-Т», кроме образов резидентных ОС СХСЗ, РС и АРМ Эмиссии, входит ПО удаленного управления «Центр-Т».

ПАК СЗИ НСД «Центр-Т» функционально организует механизм взаимодействия РС в составе системы удаленного доступа с СХСЗ, в результате чего возможно осуществлять:

- сетевую загрузку ПО на РС:
 - идентификация пользователей РС для начала работы с терминальным сервером по номерам клиентских устройств;
 - двухфакторная аппаратная идентификация пользователей РС в ПАК «Аккорд» на терминальном сервере;
 - передача образов ПО РС на РС по сети;
 - проверка целостности и подлинности полученного образа Клиентом;
- централизованное администрирование:
 - сборка образов ПО РС;
 - сопоставление образов ПО РС учетным записям пользователей;
 - настройка сетевых параметров;
 - резервирование баз данных и настроек СХСЗ и Клиента;
 - восстановление ПО «Центр-Т» из резервных копий при возникновении нештатных ситуаций;
 - контроль периферийного оборудования в рамках терминальной сессии: контроль использования USB-принтеров и/или flash-накопителей информации, подключенных непосредственно к РС;
 - контроль настроек образов ПО РС;
- централизованный аудит событий:
 - регистрация действий пользователей и администраторов СХСЗ в журналах загрузки образов ПО РС и журналах активности администраторов СХСЗ;
 - регистрация пользователей и клиентских устройств.

АРМ ЗАЩИЩЕННОГО ХРАНЕНИЯ И СЕТЕВОЙ ЗАГРУЗКИ²⁾

В п. 4 и п.п. 4.3.1.3 мы уже рассказывали про «m-TruST» – специализированный микрокомпьютер с аппаратной защитой данных. На этапе производства в «m-TruST» может быть установлено ПО разного назначения, в том числе и ПО сервера хранения и загрузки ПО ТС по сети.

¹⁾ Вариант исполнения аппаратной части ПАК СЗИ НСД «Центр-Т» выбирается при заказе.

²⁾ АРМ защищенного хранения и сетевой загрузки на базе микрокомпьютера m-TruST (<https://www.okbsapr.ru/products/newharvard/ARMzhshzmTruST/>).

АРМ сетевой загрузки на базе «m-TrusT» имеет следующие преимущества по сравнению с решением на базе традиционного сервера:

- низкая стоимость;
- техническая защита от модификации ПО сервера.

При этом сохраняются достаточно высокие вычислительные характеристики.

Общий вид АРМ защищённого хранения и сетевой загрузки показан далее на рисунках 44, 45:



Рисунок 44 - АРМ CXС3. Передняя панель

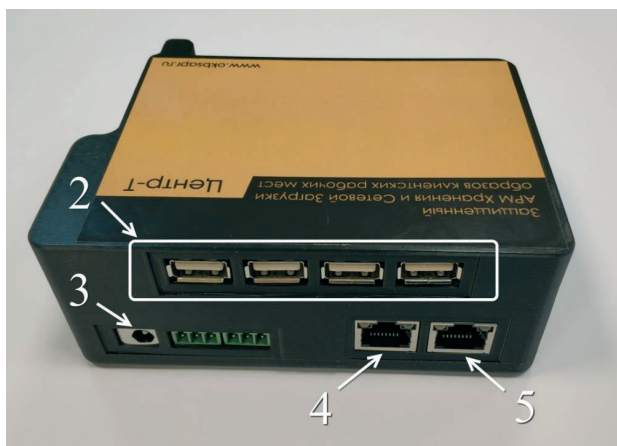


Рисунок 45 - АРМ CXС3. Задняя панель

1 – разъем mini HDMI

2 – 4 разъема USB 2.0

- 3 – разъем питания 12V, 2A
- 4 – разъем Ethernet (eth0, основной)
- 5 – разъем Ethernet (eth1)

APM защищённого хранения и сетевой загрузки реализован следующим образом: в переменную часть (сеансовую память) микрокомпьютера «m-TrusT» выделяется специальное ПО для обеспечения хранения и сетевой загрузки образов ПО на клиентские места. В этом случае загружаться переменная часть образа ОС может по технологии защищенной сетевой загрузки «Центр-Т».

Общий принцип работы APM хранения и сетевой загрузки показан рисунке 46:

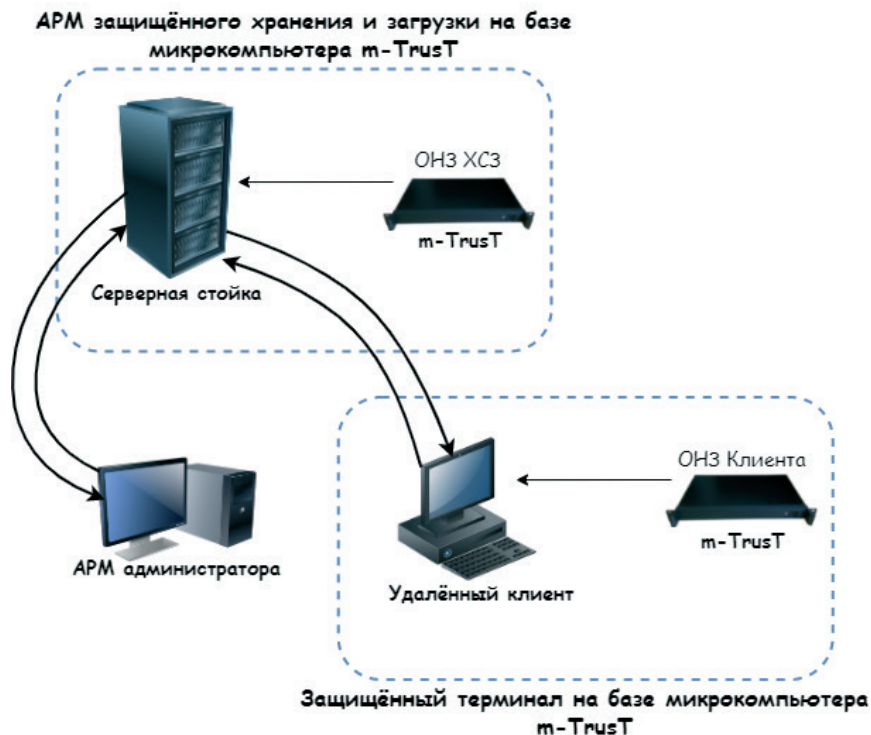


Рисунок 46 - Схема информационного взаимодействия APM CXC3 с компонентами информационной системы

Рассмотрим типовые ситуации, в которых предпочтителен выбор решения, реализующего первый или второй подход.

Главное и очевидное отличие этих двух решений, определяющее положительные и отрицательные стороны применения каждого из них в конкретных условиях эксплуатации, – и используемая аппаратная база.

Для применения решения на базе USB-устройства требуется дополнительное СБТ. Что очень важно, это СБТ должно быть совместимо со специальным встроенным ПО USB-носителя СХСЗ. В случае необходимости технической поддержки серверного компонента системы эксплуатирующая организация будет вынуждена обратиться к производителю СБТ – в одних случаях, к производителю решения для развертывания СХСЗ – в других. При разработке АРМ сетевой загрузки на базе «m-TrusT» производитель решения несет ответственность за совместимость программных и аппаратных компонентов, а обслуживание сервера выполняется одной организацией.

Если решение для СХСЗ на базе USB-устройства приобретается одновременно с необходимым для его эксплуатации СБТ, то стоимость такого комплекта будет выше стоимости АРМ сетевой загрузки на базе «m-TrusT». Но если в качестве СХСЗ используется СБТ из компьютерного парка организации (в том числе устаревшее), общая стоимость развертывания СХСЗ может быть ниже стоимости решения на базе «m-TrusT».

«m-TrusT» имеет габариты 10,5х8,5х3 см. СБТ с подключенным USB-носителем, на базе которого реализован СХСЗ из состава ПАК «Центр-Т», очевидно, будет занимать больше пространства (возможно, значительно больше). Компактный размер «m-TrusT» позволяет устанавливать его в телекоммуникационный шкаф, при этом никакие компоненты СХСЗ не будут выступать за пределы корпуса.

В случае если актуальными являются угрозы, связанные с загрузкой серверного ПО с внешних носителей, в организации, планирующей применение СХСЗ, может быть принято решение о запрете такого режима загрузки сервера в принципе. В этом случае применение решения для СХСЗ на базе USB-устройства становится невозможным. Выбор АРМ сетевой загрузки на базе «m-TrusT» позволит развернуть сервер сетевой загрузки с необходимым функционалом и при этом соответствовать предъявленному требованию.

Таким образом, АРМ сетевой загрузки на базе «m-TrusT» может рассматриваться как предпочтительный вариант, когда:

- производится проектирование или модернизация системы терминального доступа;
 - имеет значение размер оборудования (например, предполагается установка СХСЗ в телекоммуникационный шкаф);
 - нет возможности выделения отдельного СБТ для развертывания СХСЗ;
 - желательно упрощение технической поддержки оборудования;
 - запрещена загрузка сервера сетевой загрузки с внешнего носителя.
- Соответственно, выбор СХСЗ на базе USB-устройства может быть предпочтительнее, когда:
- для развертывания СХСЗ предполагается использование СБТ из компьютерного парка организации;
 - габаритные размеры оборудования и порядок технической поддержки оборудования не имеют значения;
 - загрузка сервера сетевой загрузки с внешнего носителя не запрещена.

СУЦУ СЗИ от НСД «Аккорд»

СУЦУ СЗИ от НСД – система удаленного централизованного управления средствами защиты информации от несанкционированного доступа «Аккорд»¹⁾.

СУЦУ обеспечивает централизованный сбор и хранение информации о зарегистрированных событиях доступа к ПКО и возможность централизованного управления средствами защиты информации от несанкционированного доступа «Аккорд», установленных на ПКО.

СУЦУ информирует персонал о попытках несанкционированного доступа и предоставляет единую точку контроля доступа к периферийным устройствам и контроля использования отчуждаемых машинных носителей.

СУЦУ обеспечивает централизованный мониторинг событий информационной безопасности, централизованно управляет подконтрольными объектами (компьютерами сотрудников) и средствами защиты информации от несанкционированного доступа «Аккорд», которые также разработаны компанией ОКБ САПР.

СУЦУ поддерживает ролевую инфраструктуру (7 ролей!), каждая отдельная роль обладает специфическим набором возможностей (функций), нехарактерных для других ролей. СУЦУ обеспечивает управление ролями и учетными записями персонала.

Разумеется, если такое разделение обязанностей не предусмотрено штатным составом организации, на несколько ролей может быть назначен один и тот же сотрудник, однако это решение должно быть продуманным и описанным.

¹⁾ СУЦУ (<https://www.okbsapr.ru/products/management/remote/>).

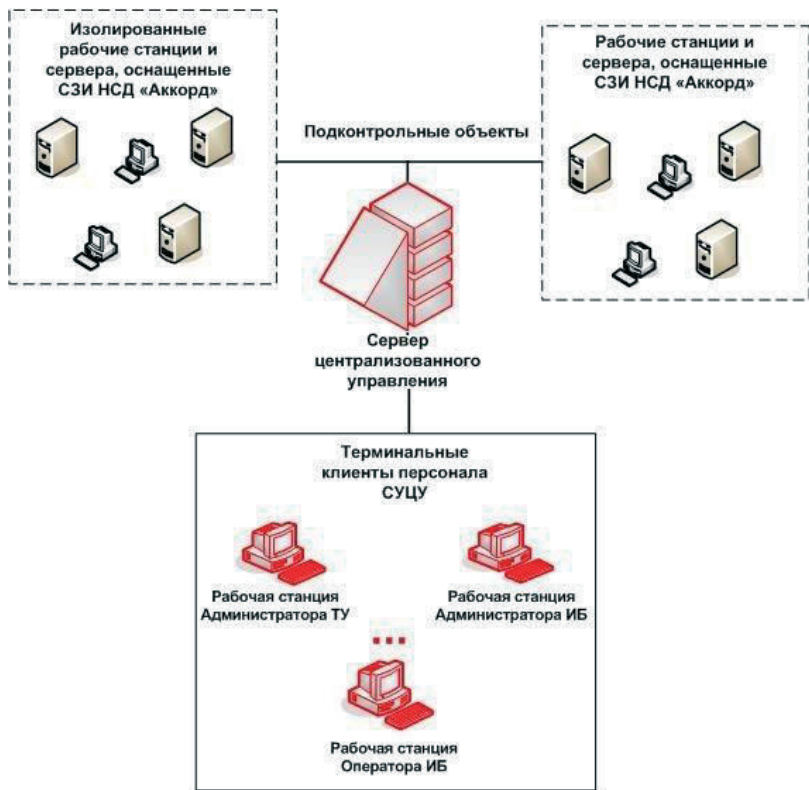


Рисунок 47 – Схема взаимодействия СУЦУ СЗИ от НСД

СУЦУ обеспечивает возможность интеграции с продуктами типа Business Intelligence – в частности, с Tivoli, есть положительный опыт интеграции с продуктом Contour BI. Такая интеграция позволяет быстро создавать отчеты для анализа конечными пользователями (руководителями организаций или подразделений, администраторами ИБ и т.д.), выполнять анализ данных журналов событий средств защиты «Аккорд» совместно с анализом журналов работы других систем, одновременно функционирующих в компьютерной системе, например, системы контроля доступа, антивирусной защиты или какого-либо прикладного программного обеспечения. По запросу может быть выполнена интеграция с целевым BI.

В СУЦУ также имеется возможность интеграции с системой контроля и управления доступом СКУД.

СУЦУ СЗИ от НСД позволяет:

- управлять техническими средствами;
- осуществлять централизованный сбор и хранение информации о зарегистрированных событиях доступа к подконтрольным объектам;

- выполнять централизованное управление средствами защиты информации от несанкционированного доступа на подконтрольных объектах;
- управлять списком зарегистрированных подконтрольных объектов
- управлять доступом к коммутационным портам и периферийным устройствам.

ПАСПОРТ ПО

Для систематической (а также и внезапной, вне расписания) проверки состава ПО на рабочих местах предназначен программный продукт «Паспорт ПО»¹⁾, с помощью которого для каждого рабочего места создается и периодически проверяется «паспорт», в котором отражен перечень установленного ПО и его характеристики.

Основные элементами ПМ «Паспорт ПО» являются сервер с базой данных, компонент управления (автоматизированное рабочее место – АРМ – управления), клиентский компонент, устанавливаемый на подконтрольные объекты (ПКО), сервис обмена сообщениями RabbitMQ, обеспечивающий взаимодействие по сети между всеми элементами:

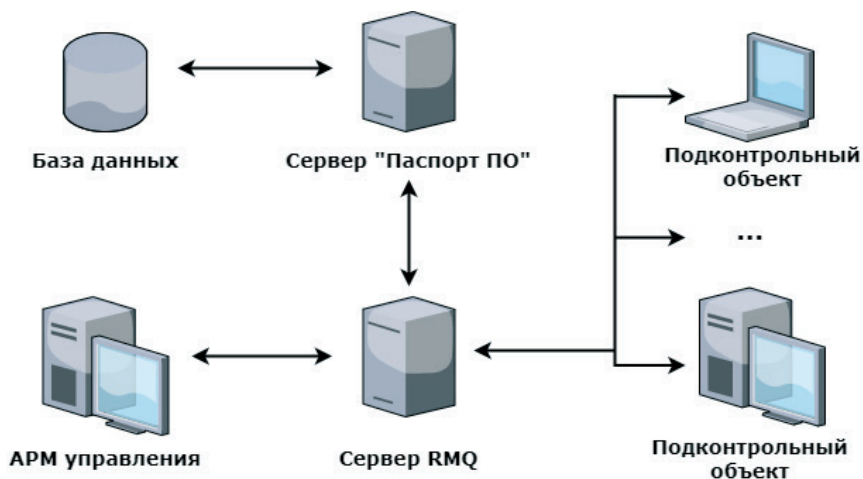


Рисунок 48 - Основные элементы ПМ «Паспорт ПО»

Применение «Паспорт ПО» решает проблему контроля за установкой ПО на рабочих местах пользователей в крупных и территориально распределённых системах.

К числу основных функций «Паспорт ПО» относятся:

- управление пользователями и их правами доступа в рамках «Паспорт ПО»;
- настройка состава опроса ПКО;
- настройка расписания опроса ПКО;

¹⁾ «Паспорт ПО» (<https://www.okbsapr.ru/products/management/software-passport/>).

- фиксация результатов опроса в виде подписи проекта «паспорта»;
- сравнение результатов опроса между собой.

«Паспорт ПО» позволит избежать таких неприятных явлений, как:

- нерациональное использование рабочего времени (сотрудники играют в онлайн игры или решают свои, не связанные со служебными, задачи);
- угрозы безопасности и промышленный шпионаж (устанавливаться инициативными пользователями могут потенциально опасные или заведомо вредоносные программы);
- нарушение работоспособности системы и/или непрерывности бизнес-процессов (вирусные заражения или рассинхронизация версий функционального программного обеспечения, которая может приводить (и часто приводит) к потере совместимости – невозможности совместной обработки файлов и баз данных, подлежащих совместной обработке, и тому подобное).

Для своевременного обнаружения и предотвращения несанкционированных изменений недостаточно организационных мер (инструкций, регламентов), необходим постоянный мониторинг состояния рабочих мест пользователя, который и обеспечивает решение «Паспорт ПО».

Принцип, положенный в основу продукта «Паспорт ПО», соответствует принципу управления конфигурациями, ориентированному на безопасность (Security-Focused Configuration Management of Information Systems, SecCM) – одной из концепций повышения защищённости информационной системы за счёт управления её конфигурациями.

Принцип SecCM указывает основные шаги, выполнение которых позволяет реализовать корректное управление конфигурациями в информационной системе. Так, ключевыми этапами являются: планирование SecCM (разработка политик применения средства SecCM), внедрение SecCM (определение базовых конфигураций и их утверждение), контроль изменений конфигурации (использование некоторой панели управления конфигурации для рассмотрения и утверждения изменений в ИС) и мониторинг уже утверждённых конфигураций.

«Паспорт ПО» предназначен для автоматизации контроля целостности состояния программной среды (основных характеристик файлов программного обеспечения) и контроля изменений состава ПО (установленные на средство вычислительной техники системные и прикладные программные продукты). Фиксация состояния конфигурации СВТ (программной среды вместе с совокупностью состава ПО) выполняется через создание записей специального вида – проектов паспортов ПО. Заверенный проект паспорта называется паспортом ПО и представляет эталонное состояние конфигурации СВТ. Для формирования паспорта ПО пользователь должен обладать в рамках «Паспорт ПО» правом на подпись проекта.

4.3.2.2 Защищённые специальные носители

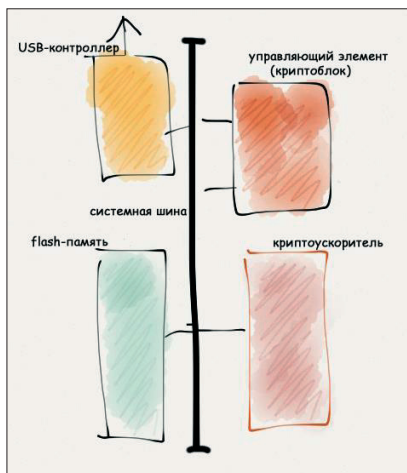
Использование личных устройств пользователей в рабочем процессе сопряжено с проблемой утечки информации – на флешки и токены можно легко копировать

корпоративную информацию и вынести её за пределы организации. К тому же флешки можно легко потерять, их могут украсть или отобрать (с применением силы или методов социальной инженерии, например).

Проконтролировать использование личных устройств практически нельзя. Можно запретить использовать персональные носители в пределах организации, но это может привести к росту недовольства среди сотрудников и никак не решит проблему утечки информации, связанной с потерей и кражей этих устройств.

Самым приемлемым решением является использование в организации носителей информации, обладающих усовершенствованной архитектурой. Такие устройства должны быть менее универсальными, чем обычные флешки, и выполнять лишь заданное количество функций и только на тех компьютерах, на которых использование устройств разрешено, а также не должны ничего выполнять при любых других условиях.

Служебные носители (СН) «Секрет»¹⁾ ОКБ САПР обладают усовершенствованной архитектурой (см. рис. 49). Управляющий элемент в СН «Секрет» различных модификаций реализован по-разному, однако общая логика остается единой: управляющий элемент



«коммутирует» компьютер с диском «Секрета» (собственно флешкой) только после успешного завершения контрольных процедур: взаимной аутентификации СН, компьютера и пользователя. До того, как сценарий аутентификации будет успешно разыгран до конца, диск «Секрета» не будет примонтирован, не появится в списке дисков и не окажется доступен не только для пользователя, но и для системы (с ее потенциальными закладками или вирусами).

Рисунок 49 - Служебный носитель «Секрет»

Дополнительно защитные свойства «Секрета» могут быть усилены посредством реализации технологических мер защиты от атак, связанных с несанкционированным изменением структуры аппаратного модуля. Выбирать такой носитель целесообразно тогда, когда разумно предположение, что злоумышленник может попытаться считать данные с флеш-памяти напрямую, например, выпаяв ее с устройства.

Под данной формулировкой имеется в виду защита данных посредством «прозрачного» шифрования. Однако реализованный в СН «Секрет» метод «прозрачного» шифрования с нормативной точки зрения шифрованием не является. По определению шифрование данных это процесс перевода незашифрованных данных в зашифрованные с помощью секретного ключа. Пользователь (или программа) зашифровывает информацию с помощью секретного ключа для последующей её передачи либо хранения. Расшифровать зашифрованные данные может лишь

¹⁾ Что делает флешку «Секретом»? (<https://www.okbsapr.ru/products/storage/flash/what-makes-a-secret/>).

ограниченный круг пользователей (либо программ), которые имеют доступ к этим данным. Целью шифрования данных является ограничение доступа пользователей (или программ) к этим данным.

В «Секретах» с «прозрачным» шифрованием владельцами секретного ключа являются не пользователи (или программы), а сами СН. Целью шифрования данных в «Секретах» является не ограничение круга пользователей (или программ), которые могут получить доступ к данным, а ограничение круга способов, с помощью которых можно эти данные прочесть. При этом данные на СН зашифровываются с помощью ключа и расшифровываются по его предъявлению. С нормативной точки зрения реализованный в «Секретах» метод шифрования шифрованием не является. Хотя с точки зрения математики это и есть шифрование, так как условие «зашифрует-расшифрует» с помощью ключа выполняется. Поэтому реализованный в «Секретах» метод «прозрачного шифрования» ОКБ САПР условно называет «шифрованием».

На базе технологии различения своих/чужих компьютеров «Секрет» построены следующие продукты:

– семейство	защищенных	съемных	носителей:
ПАК «Секрет Особого Назначения»,	ПАК «Секрет	Фирмы»,	ПАК «Секрет
Администратора»;			

- носители ключевой информации (ПАК «Идеальный токен»);
- средства архивирования журналов (ПАК «ПАЖ»);
- отчуждаемый шлюз (ПАК «Система Ниппель»).

Далее в двух словах о каждом.

ЗАЩИЩЁННЫЕ ФЛЕШКИ «СЕКРЕТ»

«Секрет Особого Назначения»

Бывает так, что данные, конфиденциальность которых должна контролироваться, должны храниться на служебном носителе и переноситься сотрудником в рамках его должностных обязанностей на различные компьютеры, в том числе и за пределы информационной системы организации.

ПАК «Секрет Особого Назначения»¹⁾ – защищенный носитель, флешка, который может использоваться на любом компьютере, разрешенным администратором, не важно, находится ли он в корпоративной сети. Главные защитные функции СН – это ограничение числа компьютеров, на которых разрешено использование устройства и ведение аппаратного журнала событий, в котором фиксируются все попытки работы с СН на различных компьютерах, вне зависимости от того, была ли попытка успешной.

Диск «Секрета Особого Назначения» имеет два раздела – открытый (но защищенный от записи) и защищенный (но доступный для записи после примонтирования).

¹⁾ Секрет Особого Назначения (<https://www.okbsapr.ru/products/storage/flash/secret/special/>).

При первом подключении «Секрета» к компьютеру монтируется открытый раздел диска СН. Администратор устройства, посредством ПО, стартующего с открытого раздела диска СН, выполняет настройки политики использования СН и процедуру добавления компьютеров в список разрешенных, по завершении которых устройство передается непосредственному пользователю.

Пользователь СН выполняет процедуру регистрации, в результате которой формируется пароль, необходимый для получения доступа к закрытому разделу диска устройства.

При каждом последующем подключении управляющий элемент устройства определяет соответствие или несоответствие компьютера параметрам тех, что находятся в списке разрешенных.

Если параметры совпадают, то запрашивается пароль пользователя. После успешного завершения процедуры авторизации, монтируется закрытый раздел диска «Секрета».

Если проверки не увенчались успехом (пользователь ввел некорректный пароль или в ходе проверки управляющий элемент выявил несоответствие компьютера параметрам разрешенных), то в доступе будет отказано: закрытый раздел диска СН не будет примонтирован. Другими словами, на любом компьютере, кроме тех, что явно разрешены администратором, флешка не будет доступна ни на чтение, ни на запись (то есть не станет ни каналом утечки, ни каналом поступления в систему нежелательного ПО).

В «Секрете Особого Назначения» с «шифрованием», скорость чтения/записи довольно мала.

Существуют особые модификации «Секрета Особого Назначения»: «Быстрый Секрет» и «Секрет руководителя».

В некоторых случаях пользователи готовы использовать «Секрет» без «шифрования», лишь бы только привычные действия выполнялись быстрее. Для этих случаев есть отдельное решение – «Быстрый Секрет», его скорость отличается от обычного чтения/записи через USB.

В «Секрете Руководителя» имеется возможность временного отключения всех запретов и разрешения подключения к неограниченному кругу компьютеров благодаря наличию встроенных часов реального времени (RTC). Это необходимо в тех случаях, когда для сотрудников не уместен или невозможен порядок, при котором для изменения режима доступа необходимо обращаться к администратору – в таком случае имеется возможность снятия запретов на использование устройства на некоторое время, по истечении которого прежние ограничения на подключение СН снова вступают в силу.

Специальные механизмы работы СН отмечены далее в таблице 2:

Таблица 2 - Специальные функции защищённых флешек «Секрет Особого Назначения», «Быстрый Секрет», «Секрет Руководителя»

Защищённый носитель	Назначение носителей	Общие функции носителей	Специальные функции носителей
---------------------	----------------------	-------------------------	-------------------------------

ПАК «Секрет Особого Назначения»	Защищенные флешки, которые позволяют ограничить число компьютеров, на которых разрешено использование устройства, и ведут журнал событий, в котором фиксируются все попытки работы с СН. СН реализуются на базе служебного носителя с механизмами защиты от атак, связанных с несанкционированным изменением структуры аппаратного модуля. Могут реализовываться и без реализации данных мер. Предназначены как для личного, так и для корпоративного использования.	✓ настройка администратором правил доступа пользователя к информации на СН; ✓ создание «белого» списка рабочих станций (на которых разрешено работать с СН); ✓ поддержка ролей администратора, пользователя; ✓ аннулирование регистрации пользователя; ✓ разблокировка СН; ✓ общий сброс СН; ✓ ведение журнала событий.	
ПАК «Быстрый Секрет»			✓ увеличенная скорость чтения/записи.
ПАК «Секрет Руководителя»			✓ встроенные часы реального времени.

«Секрет Фирмы»

ПАК «Секрет Фирмы»¹⁾ представляет собой корпоративное решение, позволяющее получать доступ к данным, хранящимся в «Секрете», только на заранее определенных компьютерах в рамках локальной сети предприятия, находящихся в on-line связи с Сервером Аутентификации (СА).

Служебные носитель (СН) – то есть собственно «Секреты» пользователей «эмитируются» на специальном АРМ Эмиссии из состава комплекса непосредственно в эксплуатирующей организации, а покупаются они нейтральными. При этом нейтральные, неэмитированные «Секреты», или «Секреты, эмитированные для других фирм, в принципе не смогут быть зарегистрированы в системе организации.

Перед использованием СН регистрируется на СА локальной сети, на компьютерах которой предполагается использование СН.

¹⁾ Секрет Фирмы (<https://www.okbsapr.ru/products/storage/flash/secret/firm/>).

В процессе регистрации происходит обмен аутентификационной информацией между СН и СНСА, подключенным к СА (СА работает только при подключенном специальном носителе Сервера аутентификации – СНСА). Аутентификационная информация СА сохраняется на СНСА, что позволяет обеспечить учет и контроль ее использования.

Далее после успешного выполнения регистрации СН администратор подготавливает устройство к дальнейшей работе: формирует списки доступа – списки компьютеров, на которых разрешено или запрещено использование «Секрета», и настраивает сетевые параметры.

Чтобы процедура получения доступа к СН стала возможной, до начала использования СН администратор выполняет загрузку ключевой информации СНСА в сервис сервера аутентификации.

После этого устройство передается непосредственному пользователю.

Пользователь СН выполняет процедуру регистрации, в результате которой формируется пароль, необходимый для получения доступа к диску устройства.

При последующих подключениях монтирование флеш-диска «Секрета» выполняется только в том случае, если выполняются условия:

- рабочая станция получила от Сервера Аутентификации подтверждение, что «Секрет» разрешен для работы на ней;
- пользователь ввел верный PIN-код, подтвердив свое право использовать «Секрет»;
- СА подтвердил права пользователя и «Секрета».

В случае невыполнения хотя бы одного из вышеперечисленных условий диск «Секрета» не примонтируется, доступ к содержимому СН будет закрыт.

Администратор может активировать фильтр USB-носителей, входящий в состав ПО. Он блокирует использование на ПК других USB-носителей.

Для случаев, когда необходимо использовать СН в другом сегменте сети, предусмотрена процедура вторичной регистрации, своего рода «выдача мандата».

Специальные механизмы работы СН отмечены далее в таблице 3:

Таблица 3 - Специальные функции защищённых флешек «Секрет Фирмы»

Защищённый носитель	Назначение носителя	Основные функции носителя
ПАК «Секрет Фирмы»	Защищенные флешки «Секрет Фирмы» позволяют ограничить число компьютеров, на которых разрешено использование устройства, и ведут журнал событий, в котором фиксируются все попытки работы с СН.	✓ двусторонняя аутентификация СН (относительно рабочей станции и Сервера аутентификации); ✓ настройка администратором правил доступа пользователя к информации на СН;

	СН реализуются на базе служебного носителя с механизмами защиты от атак, связанных с несанкционированным изменением структуры аппаратного модуля. Могут реализовываться и без реализации данных мер. Предназначен для корпоративного использования.	✓ создание «белого» списка рабочих станций (на которых разрешено работать с СН); ✓ поддержка ролей администратора, пользователя; ✓ аннулирование регистрации пользователя; ✓ разблокировка СН; ✓ общий сброс СН; ✓ ведение журнала событий; ✓ фильтр USB-устройств; ✓ эмиссия СН (привязка СН к информационной системе отдельной организации).
--	---	---

«Секрет Администратора»¹⁾

Нередко случается так, что ПО, установленное на компьютере (к примеру, файлы ОС, различные приложения, антивирусные базы и прочие обновления), перестает должным образом работать: отказывает совсем или работает некорректно.

В целях поддержки бесперебойной работы компьютеров и обеспечения целостности ПО целесообразно иметь под рукой набор эталонных образов ПО, защищенный от и несанкционированного изменения и подготовленный для незамедлительного применения в случае возникновения нештатных ситуаций (сбоев в системе, прекращения электропитания, атаки вредоносного ПО и т.д.).

ПАК «Секрет Администратора» - защищенный носитель информации, построенный по технологии «Секрет», предназначенный для защиты эталонных образов ПО от несанкционированных модификаций и поддержания автоматизированных систем организации в работоспособном состоянии.

Механизм работы СН реализован так, что предусмотрена возможность задания режима доступа «чтение и запись» к СН на АРМ администратора ИБ и режима доступа «только чтение» на компьютерах пользователей либо компьютерах сегмента сети.

¹⁾ Секрет Администратора (https://www.anti-malware.ru/analytics/Threats_Analysis/How-to-deal-with-human-factor#part63).

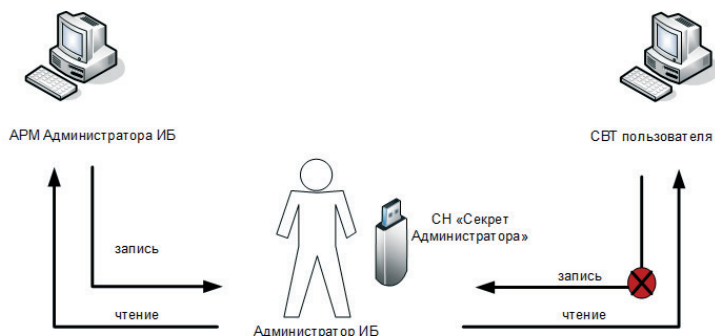


Рисунок 50 - Пример работы СН «Секрет Администратора»

При последующих подключениях СН к компьютеру после успешного прохождения процедур аутентификации и идентификации пользователем (либо администратором ИБ) посредством механизма разграничения доступа, реализованного в СН, разрешается (или запрещается) доступ к памяти и функциям СН в соответствии с назначенным режимом доступа. Достигается попутно еще один эффект – исключение неконтролируемого тиражирования, приобретенного организацией ПО за ее пределы (на посторонних компьютерах диск не откроется и на чтение).

Специальные механизмы работы СН отмечены в таблице 4:

Таблица 4 - Специальные функции СН «Секрет Администратора»

Защищённый носитель	Назначение носителя	Основные функции носителя
ПАК «Секрет Администратора»	Служебный носитель с управляемыми атрибутами доступа к памяти – RO, RW, AO. Предназначен для хранения и переноса эталонных образов ПО.	✓ создание «белого» списка рабочих станций (на которых разрешено работать с СН); ✓ разблокировка СН; ✓ общий сброс СН; ✓ ведение журнала событий; ✓ управление доступом к flash-памяти СН; ✓ механизм проверки контрольных сумм эталонных образов ПО.

НОСИТЕЛИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Токен как часть криптографического средства защиты, функционирует в некоторой среде, которая складывается из технических и программных средств, образующих среду функционирования криптографического средства и способных повлиять на выполнение им собственных функций. Использование технических и программных средств порождает объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы безопасности информации. Очевидно, что ограничение доступа к ключу только использованием PIN-кода недостаточно. Токен должен использоваться только в той системе, в которой обеспечена защита от несанкционированного доступа (а значит, обеспечена доверенная среда функционирования криптографического средства), а PIN-код можно правильно ввести в любой среде.

Один из способов гарантировать использование криптографической информации в пределах четко выделенной доверенной среды функционирования криптографического средства – ограничение числа компьютеров, на которых технически возможна работа с токеном.

ПАК «Идеальный токен» (ИТ) – это токен, который по технологии «Секрет» различает разрешенные для работы компьютеры и не работает на остальных. Действия с ключом пользователь может выполнить только на тех компьютерах, которые разрешены администратором, что снижает риск компрометации ключей при подключении к недоверенным компьютерам¹⁾.

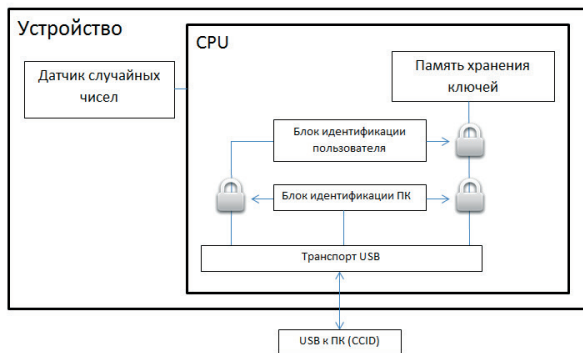


Рисунок 51 – Архитектура ПАК «Идеальный токен»

До начала использования ИТ на компьютер устанавливается специальное ПО (внешнее по отношению к «Идеальному токenu»).

При первом подключении ИТ к компьютеру регистрируется администратор устройства. После этого администратор выполняет процедуры добавления компьютеров в список разрешенных и начального форматирования устройства, по завершении которых устройство передается непосредственному пользователю.

¹⁾ Идеальный токен (<https://www.okbsapr.ru/products/storage/auth/idealtoken/>).

Получив ИТ, пользователь проворит процедуру регистрации, в результате которой формируется PIN-код, необходимый для получения доступа к устройству.

При каждом последующем подключении блок идентификации ПК (имеется в виду идентификация устройством компьютера) определяет параметры текущего компьютера и сравнивает их с теми данными, которые были получены при добавлении компьютера в список разрешенных.

Если параметры совпадают, то разрешается доступ к токenu со стороны внешнего ПО – то есть со стороны средства криптографической защиты информации.

После успешного завершения проверок блока идентификации ПК управление устройством передается блоку идентификации пользователя, который, в случае ввода корректного PIN-кода пользователем, разрешает доступ к памяти ИТ.

Если же в ходе проверки блок идентификации ПК выявил неразрешенный для использования ИТ компьютер или процедура авторизации завершилась неудачей, то в доступе будет отказано.

Стоит отметить, что с точки зрения безопасного существования криптографических ключей в автоматизированной системе (АС) принципиальное значение имеют 2 фактора:

- защищенное хранение ключа (и, соответственно, носитель ключа);
- условия доступа к ключу и работы с ним (то есть среда функционирования криптографии (СФК)).

ПАК «Идеальный токен» обеспечивает защищенное хранение ключа и доверенную СФК, так как:

- является персональным отчуждаемым устройством,
- является специализированным именно для хранения ключей устройством (то есть обеспечивает возможность защищенного хранения криптографических ключей с применением интерфейсов работы со смарт-картой (CCID или PKCS#11)),
- предоставляет доступ к ключам только легальному пользователю после успешной аутентификации в устройстве,
- предоставляет легальному пользователю доступ к ключам только на тех СВТ, на которых данному пользователю разрешено работать с данным ключевым носителем.

Специальные механизмы работы ПАК «Идеальный токен» отмечены в таблице:

Таблица 5 - Специальные функции ПАК «Идеальный токен»

Защищённый носитель	Назначения носителя	Основные функции токена
ПАК «Идеальный токен»	Предназначен для хранения и переноса ключевой информации.	✓ создание «белого» списка рабочих станций (на которых разрешено работать с СН);
	Токен с функцией ограничения числа разрешенных для	✓ хранение криптографических

	использования компьютеров, используется для хранения криптографических ключей и их применения на ПК, разрешенных администратором ИБ.	ключей на разрешенных администратором ПК; ✓ разблокировка СН; ✓ поддержка ролей администратора, пользователя; ✓ применение криптографических ключей на ПК, разрешенных администратором.
--	--	--

СРЕДСТВА АРХИВИРОВАНИЯ ЖУРНАЛОВ

Накопитель, «различающий» компьютеры, полезен также администратору системы, собирающему журналы событий с разных рабочих станций для их последующего раздельного хранения. Запись журналов с разных ПК на один носитель в дальнейшем может привести к путанице при попытке анализа, а вероятность перепутать носители при сборе журналов и случайно записать журнал с ПК в архив с другого – очень велика.

ПАК «ПАЖ» – программно-аппаратный непerezаписываемый служебный носитель информации – устройство, предназначенное для записи и защищенного хранения журнала событий. Помимо этого, «ПАЖ» может применяться для архивирования любых необходимых для неприкосновенного хранения данных¹⁾.



Рисунок 52 – ПАК «ПАЖ»

Благодаря настраиваемым политикам, «ПАЖ» позволяет записывать на себя данные со строго определенных (разрешенных администратором) компьютеров, что дает

¹⁾ ПАЖ (<https://www.okbsapr.ru/products/storage/data/pazh/>).

возможность не смешать необходимые журналы с файлами журналов других (неразрешенных) компьютеров.

Память устройства «ПАЖ» находится в режиме Add only, то есть в нее можно только добавлять, а что-либо удалять или изменять в ней – нельзя.

При первом подключении СН к компьютеру выполняется монтирование открытого раздела диска СН в режиме «только чтение».

Затем выполняется процедура регистрации администратора и пользователя устройства. Администратор, в свою очередь, создает список разрешенных компьютеров, с которых, в последствии, возможно копирование журналов приложений на закрытый раздел диска «ПАЖ».

При последующих подключениях «ПАЖ» монтирование закрытого раздела диска происходит только после успешной авторизации пользователя устройства и только при условии соответствия компьютера параметрам тех, что находятся в списке разрешенных.

При этом доступ к закрытому разделу диска СН открывается в режиме «только чтение».

Специальные функции ПАК «ПАЖ» показаны в таблице 6:

Таблица 6 – Специальные функции ПАК «ПАЖ»

Назначение носителя	Основные функции носителя
Служебный носитель с управляемыми атрибутами доступа к памяти – RO, RW, AO. Предназначен для хранения и переноса журналов событий ИБ.	✓ создание «белого» списка рабочих станций (на которых разрешено работать с СН); ✓ разблокировка СН; ✓ общий сброс СН; ✓ ведение журнала событий; ✓ поддержка ролей администратора, пользователя, аудитора; ✓ аннулирование регистрации пользователя и аудитора; ✓ предоставление возможности записи событий в журнал только на разрешенных РС; ✓ предоставление возможности чтения событий из журнала только на разрешенных РС; ✓ механизм контроля доступа к flash-памяти СН.

ОТЧУЖДАЕМЫЙ ШЛЮЗ¹⁾

Общеизвестные средства защиты, как правило, контролируют только те информационные потоки, которые проходят по каналам, предназначенным для их

¹⁾ Отчуждаемый шлюз (https://www.anti-malware.ru/analytics/Threats_Analysis/How-to-deal-with-human-factor#part66)

передачи. Подобный подход оставляет возможность обмена информацией посредством скрытых каналов (СК) – непредусмотренных коммуникационных каналов, которые могут быть использованы для нарушения политики безопасности.

Одним из методов противодействия опасным СК является использование однонаправленного канала передачи данных – механизма, позволяющего в целях обеспечения безопасности информации осуществлять передачу данных только в одном направлении.

ПАК «Система Ниппель» представляет собой отчуждаемый шлюз, построенный по технологии «Секрет» и предназначенный для организации однонаправленного канала передачи данных с целью защиты автоматизированных систем (АС) от нежелательного и неавторизованного раскрытия обрабатываемой, хранимой и передаваемой в АС информации конфиденциального характера.

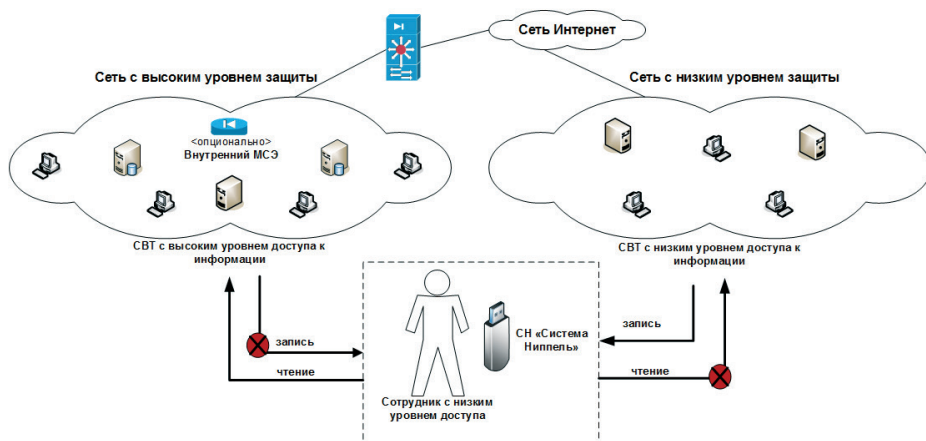


Рисунок 53 - Пример организации одностороннего канала передачи данных посредством СН «Система Ниппель»

Для реализации однонаправленного канала передачи данных предусмотрена возможность задания режима доступа («только чтение», «только запись», «чтение и запись») к СН для обособленного компьютера или сегмента сети.

В этом случае при регистрации СН в сегменте сети с низким уровнем защищенности для него устанавливается режим «чтение и запись» или «только запись», а при регистрации в сегменте сети с высоким уровнем защищенности – «только чтение». При таких параметрах доступа у пользователя не будет возможности копирования информации высокого уровня доступа и переноса ее в сегмент сети с низким уровнем доступа.

При последующих подключениях СН к СВТ после успешного прохождения процедур аутентификации и идентификации пользователем посредством механизма разграничения доступа, реализованного в СН, разрешается (или запрещается) доступ к памяти и функциям СН в соответствии с назначенным режимом доступа.

Специальные механизмы работы ПАК «Система Ниппель» отмечены в таблице 7:

Таблица 7 – Специальные функции ПАК «Система Ниппель»

Назначение носителя	Основные функции носителя
Служебный носитель с управляемыми атрибутами доступа к памяти – RO, RW, АО.	✓ создание «белого» списка рабочих станций (на которых разрешено работать с СН); ✓ разблокировка СН; ✓ сброс СН;
Предназначен для организации однонаправленного канала передачи данных.	✓ ведение журнала событий; ✓ поддержка ролей администратора, пользователя; ✓ аннулирование регистрации пользователя; ✓ управление доступом к flash-памяти СН; ✓ настройка временного интервала работы с СН.

4.3.3 Специальные инструменты для управления встроенными механизмами безопасности

В ряде ОС имеются встроенные инструменты безопасности такие, как, например, функция управления USB-портами. «Управление» в отношении этого механизма – некоторое преувеличение, в общем случае, у него есть два состояния:

1. он включен, и тогда все USB-порты компьютера работают в режиме «только чтение»;
2. он отключен, тогда все USB-порты работают штатным образом.

Возможность такого ограничения USB-портов присутствует как в ОС семейства Windows, так и в ОС семейства Linux. К примеру, в ОС Windows управлять USB-портами возможно несколькими способами: настроить групповые политики управления доступом к USB-носителям (с помощью настроек GPO) или же изменить настройки параметров доступа к различным классам USB-устройств в реестре, или изменить параметры настройки драйвера USB Storage Driver. В ОС Астра Linux управлять USB-устройствами можно, например, применяя механизм parsec devices access control (pdac).

Как и любая функция или настройка, реализованная в ОС, функция контроля USB-портов может быть несанкционированно отключена (специально, или из-за системного сбоя, или действия вредоносных программ, например). Значит, для того чтобы использование такого механизма имело смысл, в системе должно быть какое-то средство, которое контролировало бы, включен ли механизм, и сигнализировало, если отключен.

Эта задача отличается от контроля целостности. Не достаточно убедиться, что механизм не удален и не изменен, нужно убедиться, что он включен.

Такое средство, несомненно, должно быть запущено на исполнение раньше, чем контролируемый механизм (т.е. до загрузки ОС).

Примером такого средства является программное обеспечение «USB Guard», разработанное компанией ОКБ САПР.

4.3.3.1 USB Guard. Функциональный модуль UEFI

Программное обеспечение «USB Guard. Функциональный модуль UEFI»¹⁾ (ПО «USB Guard») представляет собой комплекс программных средств, предназначенных для контроля активности механизма управления USB-портами при старте ОС. ПО предназначено для работы на CBT с ОС Астра Linux.

Основные функции ПО «USB Guard»:

- проверка наличия модулей из состава ПО «USB Guard» в ОС;
- проверка активности механизма контроля USB-портов в (pdac);
- восстановление активности механизма контроля USB-портов в случае, если он был выключен;
- блокировка ОС в случае невозможности восстановления активности механизма контроля USB-портов.

ПО «USB Guard» встраивается в BIOS CBT и функционирует в его составе.

В связи с этим до начала работы администратору CBT нужно установить «USB Guard» в BIOS CBT. Для этого необходимо:

- в настройках BIOS CBT установить загрузку ОС с USB-носителей;
- подключить USB-носитель с ПО «USB Guard» (входит в комплект поставки) к USB-порту CBT;
- после этого перезапустить CBT, дождаться автоматической перезагрузки CBT;
- повторно перезапустить CBT и снова дождаться его автоматической перезагрузки;
- затем следует отключить USB-носитель, на котором находится ПО «USB Guard», от USB-порта CBT.

Общий принцип работы ПО «USB Guard» показан далее на рисунке 54:

¹⁾ USB Guard. Функциональный модуль UEFI (<https://www.okbsapr.ru/products/spetsialnye-instrumenty/USBGuardFunktsionalnyyModulUEFI/>).

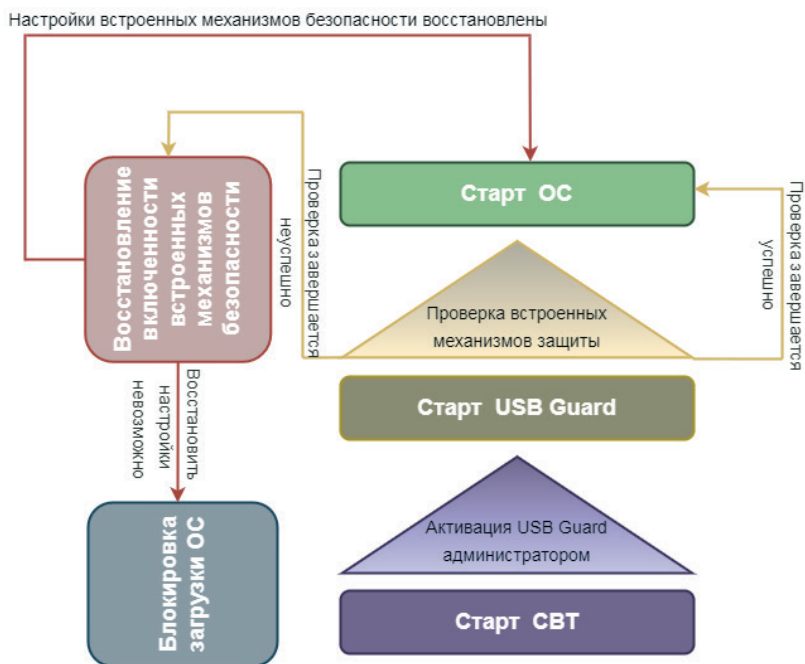


Рисунок 54 - Схема работы «USB Guard»

ПО «USB Guard» работает прозрачно для пользователя.

До работы непосредственного пользователя администратор должен выполнить настройку ПО «USB Guard» – активировать его запуск.

Для этого при старте CBT необходимо удерживать нажатой кнопку Ctrl. Наверху экрана появится окно, предлагающее перейти в режим настройки ПО «USB Guard».

```

Press Ctrl+u to start usb manager
USB guard: To enter the USB guard management Console, press Ctrl-u
-
  
```

Рисунок 55 – Переход в режим настройки ПО «USB Guard»

По нажатии комбинации клавиш Ctrl-и появится окно, в котором нужно запустить ПО «USB Guard», выбрав кнопку <Enable USB guard>.

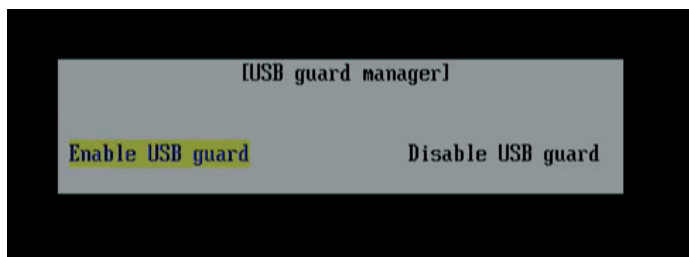


Рисунок 56 – Запуск ПО «USB Guard»

На этом настройка ПО «USB Guard» завершается. Далее при работе непосредственного пользователя «USB Guard» будет запускаться автоматически при каждом включении компьютера.

Для того чтобы пользователь сам не отключил «USB Guard», необходимо принять какие-либо организационные или технические меры, например, установить пароль на BIOS.

В дальнейшем проверка наличия и целостности собственных модулей, проверка включенности механизма контроля USB-портов, восстановление включенности или блокировка загрузки, если восстановление выполнить не удастся, выполняется при каждом запуске ОС, пока «USB Guard» сам в свою очередь не будет отключен.

Если «USB Guard» обнаружил невозможность включения подконтрольного механизма – например, если выявлено, что модули «USB Guard» в ОС повреждены или отсутствуют, загрузка ОС блокируется и может быть продолжена только с участием администратора, который проведет восстановительные процедуры.

5 ОТРАЖАЕМ КИБЕРАТАКИ

На сегодняшний день существует множество различных типов кибератак. Их цели различны, как и различны способы их совершения.

Очевидно, что кибератаки могут нанести серьёзный вред любой профессиональной деятельности. Совершаются они, в большинстве случаев, незаметно для глаз обычного пользователя, а последствия могут быть плачевными:

- утечка информации;
- компрометация персональных данных;
- перехват управления инфраструктурой организации;
- модификация сетевого трафика;
- подмена данных;
- заражение системы вредоносными программами;
- выход из строя объектов ИС и многое другое.

Далеко не всегда возможно отследить атаку, найти в системе вредоносное ПО, и тем более, выйти на нарушителя – хакера или группу хакеров, которые занимаются преступной деятельностью. В большинстве случаев злоумышленники уходят от ответа по причине невозможности их обнаружения в киберпространстве.

Выход из данной ситуации один – укреплять границы информационного пространства организации. В борьбе с кибератаками помогут только качественные, надёжные и проверенные средства защиты информации позволят противостоять кибератакам и предупредить их последствия.

Продукты компании ОКБ САПР – лучшие средства для защиты от кибератак.

Разнообразие категорий продуктов ОКБ САПР позволяет обеспечить защиту системы практически от любых угроз безопасности.

Уникальными характеристиками продукции ОКБ САПР являются:

- пошаговый механизм контроля целостности;
- усовершенствованные архитектуры комплексов;
- «вирусный иммунитет»;
- разграничение доступа на основе мандатного и дискреционного механизмов контроля доступа;
- обеспечение доверенной среды функционирования;
- централизованное управление работой пользователей и администрирование СЗИ.

В таблице 8 показаны основные тенденции развития¹⁾ кибератак за прошедший год, а также проведено сопоставление причин роста числа кибератак и решений компании ОКБ САПР, с помощью которых им можно противостоять.

¹⁾ Отчет Solar JSOC Security Report. Итоги года (https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf).

Таблица 8 - Кибератаки и как с ними бороться.

Тенденции развития кибератак	С чем связан рост кибератак	Продукты ОКБ САПР, с помощью которых возможно противостоять атакам
✓ рост числа атак с применением вредоносного ПО (шифровальщиков); ✓ рост атак на перехват управления; ✓ увеличение случаев применения фишинга; ✓ увеличение числа атак через приложения.	1. совершенствование инструментария злоумышленников.	1. средства защиты от вредоносного инструментария (п.п. 4.3.1): 1.1 средства доверенной загрузки (п.п. 4.3.1.1): • СЗИ от НСД «Аккорд-АМДЗ»; • СЗИ от НСД «ИНАФ»; • СДЗ «Аккорд-МКТ»; 1.2 средства защиты систем виртуализации (п.п. 4.3.1.2): • СПО «Аккорд-KVM»; • СПО «Аккорд-В.»; • СПО «Сегмент-В.»; 1.3 защищённые микрокомпьютеры m-TrusT (п.п. 4.3.1.3); 1.4 средства разграничения доступа (п.п. 4.3.1.4): • ПАК «Аккорд-Х»; • СПО «Аккорд-Win64 К»; • СПО «Аккорд-Х К»; 2. специальные инструменты для управления встроенными механизмами безопасности: 2.1 ПО «USB Guard» (п.п. 4.3.3.1).

	2. отсутствие контроля за работой пользователей.	1. средства контроля за работой пользователей (п.п. 4.3.2): 1.1 средства централизованного управления рабочими местами и настройками СЗИ (п.п. 4.3.2.1): • ПАК «Центр-Т»; • автоматизированное рабочее место (АРМ) защищенного хранения и сетевой загрузки на базе микрокомпьютера «m-TrusT»; • система удалённого централизованного управления «Аккорд» («СУЦУ»); • программный продукт (ПП) «Паспорт ПО»; 1.2 защищённые носители информации (п.п. 4.3.2.2): • семейство защищенных съемных носителей: ПАК «Секрет Особого Назначения», ПАК «Секрет Фирмы», ПАК «Секрет Администратора»; • носители ключевой информации (ПАК «Идеальный токен»); • средства архивирования журналов (ПАК «ПАЖ»); • отчуждаемый шлюз (ПАК «Система Ниппель»).
• рост числа атак с применением метода Brute force компрометации внутренних учетных записей	3. незащищённый удалённый доступ	1. средства защиты удалённого доступа (4.1): • средство обеспечения доверенного сеанса (СОДС) «МАРШ!» (п.п. 4.1.1); • «TrusT Удалёнка» (п.п. 4.1.2); • двухконтурный моноблок (п.п. 4.1.3); • защищённые терминалы «m-TrusT Терминал» и «Центр-TrusT» (п.п. 4.1.4); • криптошлюзы «fin-TrusT» (п.п. 4.1.5); • TrusT-in-Motion (п.п. 4.1.6).
• рост числа атак типа Supply-chain	4. популярность аутсорсинга	1. средства контроля точек подключения сторонних организаций (п.п. 4.2): • МЭ-TrusT (п.п. 4.2.1).

Компания ОКБ САПР всегда готова предоставить подробную информацию о любых своих продуктах и решениях дополнительно в любом удобном формате, а также провести демонстрацию или предоставить образец во временное пользование.

Вопросы и пожелания можно отправить, написав по адресу okbsapr@okbsapr.ru, или позвонив по телефону +7 (495) 994-72-62.