it-world.ru

10.2022 (№ 225) I октябрь 2022

i-Manager

АДМИНИСТРАТОР ИНФОРМАЦИОННЫ[illegible]ОГИЙ

СПЕЦВЫПУСК

Александр Шойтов,
заместитель министра
цифрового развития, связи
и массовых коммуникаций РФ

Кибербезопасность: от концепции к реальности

Как защитить государственные ИТ-системы, обрабатывающие информацию, содержащую государственную тайну, а также заместить иностранные решения класса ID&AM?

По оценкам аналитиков, безусловными драйверами отечественного ИТ-рынка в текущих условиях становятся увеличение спроса на решения, обеспечивающие информационную безопасность предприятий при возросших рисках кибератак, и задача замещения продуктов зарубежных вендоров. Вместе эти драйверы задают вектор развития всей отрасли. Как повысить уровень информационной безопасности организаций и снизить ресурсозатраты в условиях импортозамещения, рассказывает Григорий Куликов, директор департамента решений в сфере защиты информации Группы компаний ОТР.

ГРИГОРИЙ КУЛИКОВ,
директор департамента решений в сфере защиты информации Группы компаний ОТР

С вашей точки зрения, что наиболее важно в текущей ситуации в сфере обеспечения информационной безопасности предприятия?

С весны 2022 года наша страна и ее информационные системы и ресурсы, как государственные, так и коммерческие, находятся под беспрецедентными кибератаками. Многие оказались к этому не готовы и сейчас проводят комплексные мероприятия по аудиту и донастройке решений по защите информации. Никогда ранее операторы информационных систем не были так заинтересованы в эффективной организации защиты информации, как сейчас. Поэтому важными мероприятиями в сфере обеспечения информационной безопасности организаций сегодня являются:

1. Проведение аудита текущих решений по информационной безопасности для оценки эффективности мер защиты с учетом новых актуальных угроз.

2. Формирование дорожной карты по актуализации проектных решений по защите информации, в том числе с учетом замещения «скомпрометированных» иностранных программных и аппаратных решений.

3. Внедрение целевых решений по информационной безопасности, при необходимости — с привлечением внешних сертифицированных специалистов.

4. Проведение аттестации защищенных информационных систем предприятия.

5. Обеспечение сопровождения/эксплуатации системы информационной безопасности организации.

Реализация указанных мероприятий в кратчайшие сроки существенно снизит риски кибер-угроз и повысит надежность инфраструктуры предприятия.

Что может предложить заказчику Группа компаний ОТР по направлению информационной безопасности?

Группа компаний ОТР, обладая всеми необходимыми лицензиями ФСТЭК и ФСБ и являясь партнером ведущих отечественных вендоров решений по защите информации, готова предложить свои услуги по следующим направлениям:

- аудит информационной безопасности систем;
- проектирование интегрированных территориально распределенных систем в защищенном исполнении;
- поставка и внедрение средств защиты информации;
- управление, администрирование и сопровождение систем и средств защиты информации;
- мониторинг информационной безопасности систем.

Также в продуктовой линейке ОТР есть собственное сертифицированное решение по защите информации — это программный комплекс «ОТР. Универсальный сервер безопасности» (ОТР.УСБ) класса Identity and Access Management, который обеспечивает централизованную идентификацию и аутентификацию пользователей в приложениях, а также защиту от несанкционированного доступа со стороны нарушителей в эти приложения.

В каких случаях можно использовать продукт ОТР.УСБ?

Первое направление — это замещение иностранных решений класса Id&AM. В связи с приостановкой деятельности в РФ и поставок продуктов иностранных вендоров, таких как Oracle, IBM, Microsoft и других, многократно возрастает риск реализации угроз нарушения работы средств иностранного производства классов Id&AM — в первую очередь для информационных систем государственных учреждений и кредитно-финансовых организаций. Но и коммерческим организациям такой риск сейчас исключать нельзя.

В целях минимизации подобного риска, а также для обеспечения соответствия нормативно-правовым требованиям в области импортозамещения могут применяться наши решения, которые являются импортонезависимыми и включены в реестр отечественного ПО.

Второе направление — это создание системы защиты информации с централизацией следующих функций:

- управление учетными записями и полномочиями пользователей;
- управление доступом пользователей к ресурсам прикладных информационных систем, в том числе обеспечение единого входа в приложения.

Применение централизованных функций безопасности, которые реализует ОТР.УСБ, позволяет операторам систем:

- повысить уровень защищенности систем предприятий за счет повышения уровня интеграции функций безопасности, автоматизации процессов безопасности, снижения вероятности ошибочных действий администраторов;
- повысить удобство управления централизованными функциями безопасности, а также их масштабирования;
- снизить затраты на реализацию функций безопасности в приложениях и оценку их соответствия требованиям безопасности информации;
- снять ограничения по доработке и обновлению сертифицированных приложений, обеспечить возможности дальнейшего развития приложений.

Третье направление — это защита государственных информационных систем, обрабатывающих информацию, содержащую государственную тайну.

С весны 2022 наша страна и ее информационные системы и ресурсы, как государственные, так и коммерческие, находятся под беспрецедентными кибератаками

ОТР.УСБ имеет сертификат ФСТЭК России № 4505 (действителен до 14.01.2027), подтверждающий соответствие требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий по второму уровню доверия. Это дает возможность использовать ОТР.УСБ в информационных системах, в которых обрабатывается информация со степенью секретности «совершенно секретно», в автоматизированных системах класса защищенности 2А.ОТР.УСБ — единственное решение на рынке, предоставляющее такие возможности.

Давайте рассмотрим наглядный пример: если проводить реализацию групповых политик, допустим, на контроллере домена Samba 4, то возможно использовать протокол LDAP. Из технической документации мы видим, что ОТР.УСБ задействует этот протокол. Можем ли мы сказать, что ОТР.УСБ заменит Samba 4 или продукт от Microsoft — Active Directory?

ОТР.УСБ интегрируется со службами каталогов по протоколу LDAP в целях обеспечения синхронизации учетных записей, идентификации и аутентификации пользователей.

Контроллеры доменов реализуют гораздо больший функционал, в том числе по управлению не только пользователями, но и устройствами системы, по предоставлению необходимых инфраструктурных сервисов. Поэтому полноценно заменить Samba или Active Directory ОТР.УСБ не может, но он способен стать мастер-системой по управлению учетными записями и полномочиями пользователей, которые будут экспортироваться в службы каталогов.

С какими сторонними средствами защиты информации интегрируется продукт ОТР.УСБ?

ОТР.УСБ функционирует под управлением операционной системы Astra Linux и с ней интегрируется в части синхронизации учетных записей пользователей с каталогом Astra Linux Directory.

Также продукт может быть интегрирован с системой защиты информации Secret Net — в части автоматической установки уровня конфиденциальности сеанса доступа пользователя в приложении в соответствии с текущим уровнем конфиденциальности сеанса в операционной системе.

В части аутентификации внешних пользователей ОТР.УСБ взаимодействует с «Континентом TLS-Сервер» при входе в приложение по сертификату x.509.

В части управления потоками с использованием меток конфиденциальности на сетевом уровне согласно RFC 1108/ГОСТ Р 58256–2018 ОТР.УСБ может быть интегрирован с межсетевыми экранами, поддерживающими данную технологию.

Кроме того, наш продукт может предоставлять данные о регистрируемых событиях информационной безопасности в SIEM-системы.

Следует отметить и интеграцию ОТР.УСБ со службами каталогов: Active Directory, Astra

Linux Directory, FreeIPA — в части синхронизации учетных записей, идентификации и аутентификации пользователей.

Какие существуют примеры защищаемых с помощью ОТР. УСБ информационных систем?

Есть опыт защиты прикладных информационных систем в различных сферах и на различных программных платформах:

- системы бюджетного планирования,
- системы закупочной деятельности,
- системы финансового учета и отчетности,
- системы автоматизации финансово-хозяйственной деятельности,
- аналитические системы.

Какие преимущества дает применение ОТР.УСБ?

ОТР.УСБ обеспечивает соответствие информационных систем заказчиков требованиям в области информационной безопасности и импортозамещения, а также усиление защищенности систем заказчика за счет повышения уровня интеграции функций безопасности, автоматизации процессов безопасности, снижения вероятности ошибочных действий администраторов.

К тому же наш продукт обеспечивает удобство управления функциями безопасности, поскольку они становятся централизованными, их масштабирование и гибкие возможности как собственной кастомизации (а мы готовы дорабатывать продукты как под бизнес-кейсы конкретных информационных систем и заказчиков), так и защищаемых приложений, потому что приложения уже не требуется сертифицировать и, соответственно, нет ограничений по их развитию и обновлению.

И, наверное, не последнее, но очень важное — это снижение затрат на реализацию функций безопасности в приложениях, их сертификацию, администрирование функций безопасности, аттестацию систем заказчиков по требованиям безопасности информации.

Основываясь на вашей практике, как сейчас происходит управление доступом пользователей к ресурсам организаций?

Ситуация сейчас следующая. В государственных учреждениях и ведомствах, как правило, существует большое количество информационных и автоматизированных систем, в том числе оказывающих государственные услуги гражданам. Разработку данных систем ведут разные вендоры, интеграторы, и у каждого есть свой подход к их реализации, поэтому все приложения — разрозненные.

Кроме того, прикладные информационные системы имеют встроенные механизмы безопасности, и в соответствии с действующим законодательством в области информационной безопасности они должны быть сертифицированы ФСТЭК России. Это может быть проблемой для операторов данных информационных систем, ведь процедура сертификации подразумевает дополнительные финансовые и временны́е затраты. Среди минусов также ограничения на доработки и обновления сертифицированных приложений, большие затраты на администрирование этих функций в разрозненных приложениях, высокая нагрузка на администраторов и высокая вероятность их ошибочных действий, что в ряде случаев может приводить к реализации угроз ознакомления пользователей с данными, которые им не предназначены.

Как можно избежать этих ситуаций и улучшить управление доступом к ресурсам организации?

Наш подход как раз заключается в том, что функции безопасности необходимо централизовать и максимально автоматизировать деятельность администраторов, то есть их рутинные операции должны выполняться автоматически. Также необходимо интегрировать средства защиты разного уровня между собой, что приводит к дополнительной автоматизации процессов информационной безопасности в целом. Со всем перечисленным могут помочь наш продукт ОТР.УСБ и комплексные решения по информационной безопасности.