

УПРАВЛЕНИЕ АКТИВАМИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, А ТАКЖЕ ИХ УЯЗВИМОСТЯМИ

Ваганов Михаил Александрович

магистрант, Сыктывкарский государственный университет имени Питирима Сорокина, РФ, г. Сыктывкар

Информатизация, электронный документооборот, CRM-системы и автоматизация бизнес-процессов, если раньше данные термины были «в диковинку», то теперь повсеместно проходит информатизация – переход к работе с информацией в цифровом пространстве. Информатизация представляет собой широкое понятие, включающее множество смежных областей, свои особенности, функции, и, разумеется, множество проблем, которые необходимо решить. В данной работе мы разберемся с процессом управления активами и их уязвимостями.

Мировой опыт показал необходимость применения комплексного подхода к созданию, сопровождению, обеспечению безопасности информационных инфраструктур, независимо от того рассматриваем ли мы процесс в разрезе небольшой компании или государства. Этому способствует глобальная цифровизация всего и вся, внедрение различных сервисов, сбор и хранение колоссального объема информации.

Работоспособность информационных систем чаще всего обеспечивается отделом информационных технологий, либо вовсе одним специалистом. Обеспечение работоспособности включает в себя: резервное копирование информации, периодическое обслуживание оборудования и его учет, учитывать износ и необходимость замены оборудования, следить за многообразием операционных систем и программ, планировать возможные модернизации на следующий год, а то и несколько, учитывать и закрывать возможные уязвимости. Если все из списка делать ручным трудом, пусть даже запуская скрипты – понадобится большое количество времени и сил. Но в любом случае полученные сведения не будут должным образом оформлены. Не получится выгрузить отчет и показать руководству с целью обоснования необходимости модернизации инфраструктуры [2].

Значит нужно автоматизировать данные процессы, и для этого как раз предназначены системы управления активами и управления уязвимостями.

Что они из себя представляют данные системы? Это в первую очередь удобный способ представления информации – какие узлы есть в инфраструктуре, как долго в работе, как можно провести модернизацию парка компьютерной техники, какое программное обеспечение используется, есть ли новые версии, найдены ли какие-либо уязвимости и как их можно устранить. Такие системы позволяют выгружать отчеты, и тем самым предоставлять выбранную информацию – комплексно, что позволяет снизить трудовые и финансовые издержки к минимуму, увеличить защищенность систем и скорость реагирования на возможные проблемы [1][4].

Что представляет из себя актив в разрезе информационных технологий? Это различное оборудование (серверное, коммутационное), программное обеспечение, лицензии на право использования продуктов, а также любая информация, которая позволяет компании выполнять свою деятельность.

Управление активами необходимо для эффективного использования финансов компании. Анализ использования активов позволяет спрогнозировать и предотвратить ненужные

бизнесу издержки, например простои в работе по причине неисправности сервера. Дополнительно сокращается время проведения инвентаризаций и аудитов.

Процесс управления активами можно разделить на три этапа:

- Идентификация активов. Проводится детальная инвентаризация корпоративной сети, выделяются все объекты, которые могут быть отнесены к тем или иным активам;
- Отслеживание состояния. Активы распределяются по группам, и начинается процесс отслеживания состояния по каждому из активов.
- Обслуживание. Активы получают необходимое обслуживание в соответствии с их состоянием на определенный момент времени. Актив может быть отремонтирован, заменен, модернизирован. Все манипуляции, проведенные с активом, протоколируются, что в дальнейшем можно использовать для проведения анализа, например оценки эффективности [7].

Рассмотрев и получив примерное представление о том из каких процессов состоит управление активами можем перевести полученную информацию в представление того, как это может выглядеть в обобщенной программной реализации. Выделим три уровня. На первом мы будем работать с данными об активах, то есть состоять он будет из серверов, персональных компьютеров, ноутбуков, сетевого оборудования и так далее.

На втором уровне будем работать уже с массивом данных о каждом из активов. Например, местоположение, сведения о аппаратной конфигурации, установленном программном обеспечении.

Третий включает в себя непосредственно хранение полученного массива данных, анализ полученных данных и функционал генерации отчетов и визуализации информации в виде, удобном для понимания человеком.

В результате, объединенные три уровня в одно целое и будет являться программным обеспечением для управления активами в организации [5][6].

В современном мире нецелесообразно рассматривать управление активами отдельно от управления уязвимостями. Актив в контексте обеспечения информационной безопасности представляет собой некую сущность, которая представляет ценность для обеспечения деятельности и функционирования организации, которая является объектом атаки (с целью нарушения свойств безопасности) а также объектом защиты от атак.

Поэтому если в разрезе информационной инфраструктуры актив рассматривался как любой из объектов компании, то в разрезе безопасности, активами с уязвимостью могут быть те объекты (программно-технические средства или информационные системы в целом), которые имеют определенные недостатки (слабые места), которыми в свою очередь могут воспользоваться злоумышленники.

Поэтому, для управления уязвимостями необходимо:

- собрать информацию об активах;
- провести анализ защищенности активов;
- выявить возможные уязвимости;
- принять меры по устранению уязвимостей, либо минимизации ущерба (возможно изоляции актива). При невозможности «закрытия» уязвимости, бизнесу необходимо закладывать возможные риски и последствия от реализации уязвимости.
- Проводить периодический контроль – проверять выявленные уязвимости, оценивать эффективность мер по защите [3].

Управление активами позволяет помимо оптимизации процессов информационных технологий, также повысить общую защищенность организации и активов, поскольку управление уязвимостями является частным случаем управления активами.

Список литературы:

1. Павел Гребешков. Что такое IT-активы и как ими управлять с точки зрения затрат [Электронный ресурс] // Издание о разработке и обо всём, что с ней связано URL: <https://tproger.ru/articles/chto-takoe-it-aktivy-i-kak-imi-upravlyat-s-tochki-zreniya-zatrat> (дата обращения 14.01.2025).
2. Пролозова Т.О. УПРАВЛЕНИЕ ИТ-АКТИВАМИ В ОРГАНИЗАЦИИ // Материалы IX Международной студенческой научной конференции «Студенческий научный форум» URL: <https://scienceforum.ru/2017/article/2017031281> (дата обращения: 14.01.2025).
3. Рахметов Р. Цикл лекций по дисциплине «Автоматизация процессов управления информационной безопасностью» [Электронный ресурс] // ООО «Интеллектуальная безопасность» URL: <https://www.securityvision.ru/blog/avtomatizatsiya-protssessov-upravleniya-informatsionnoy-bezopasnostyu-aktivy-uyazvimosti-konspekty-le> (дата обращения 14.01.2025).
4. Управление ИТ активами — больше, чем инвентаризация [Электронный ресурс] // Блог консалтинговой компании по кибербезопасности «10Guards»: URL: <https://10guards.com/ru/articles/it-asset-management> (дата обращения 14.01.2025).
5. Michael Stone, Chinedum Irrechukwu, Harry Perper, Devin Wynne NIST SP 1800-5 IT Asset Management [Электронный ресурс] // Computer Security Resource Center URL: <https://csrc.nist.gov/pubs/sp/1800/5/final> (дата обращения 14.01.2025).
6. R Fauzan, V Y Pamungkas, J C Wibawa Information System for Asset Management [Электронный ресурс] // IOP Conference Series: Materials Science and Engineering, Volume 662, Issue 2. DOI 10.1088/1757-899X/662/2/022020 URL: <https://iopscience.iop.org/article/10.1088/1757-899X/662/2/022020> (дата обращения 14.01.2025).
7. What Is IT Asset Management (ITAM)? [Электронный ресурс] // Блог компании «IBM»: URL: <https://www.ibm.com/blog/it-asset-management> (дата обращения 14.01.2025).