УДК 004.01
DOI: 10.33764/2618-981X-2021-6-183-188

ПОКАЗАТЕЛИ ДЛЯ ОЦЕНКИ ОРГАНИЗАЦИИ ПО КОНТРОЛЮ ЛИЦЕНЗИОННЫХ ТРЕБОВАНИЙ И УСЛОВИЙ В ЧАСТИ ДЕЯТЕЛЬНОСТИ ПО МОНИТОРИНГУ

Геннадий Дмитриевич Мальцев
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры информационной безопасности, тел: (951)368-83-19, e-mail: gendosmal725@gmail.ru

Сергей Николаевич Новиков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, д.т.н., профессор кафедры информационной безопасности, тел: (913)923-72-34, e-mail: snovikov@ngs.ru

В статье использованы труды отечественных и зарубежных ученых в области защиты информации, безопасности информационных систем, законодательные акты и нормативные документы Российской Федерации. Цель исследования – разработать показатели для оценки организации по контролю лицензионных требований и условий в части деятельности по мониторингу. С ростом важности информации растет и количество проблем с ее защитой. Совершенствуются методы хищения информации, появляются все более новые способы ее несанкционированного получения. Поэтому проблема защиты информации прибрела особую актуальность. Способы защиты должны соответствовать требованиям, иметь лицензию и сертификаты соответствующих органов. При выполнении работы изучалась литература по теме: «Нормативно-правовая база». В работе использовались методы анализа, обобщения, сравнения, классификации. Разработка показателей для оценки организации по контролю лицензионных требований в части деятельности по мониторингу. Для больших организаций и холдинговых структур рекомендуется использовать решения от HP и IBM. Для организаций малого масштаба лучше рассмотреть решения от российских компаний Positive Technologies и Общества с ограниченной ответственностью «Иновации технологии безопасность» (ООО «ИТБ).

Ключевые слова: информация, показатели, средства защиты, безопасность, мониторинг, лицензирование, требования, нормативное регулирование

INDICATORS FOR ASSESSING THE ORGANIZATION'S CONTROL OF LICENSE REQUIREMENTS AND CONDITIONS IN TERMS OF MONITORING ACTIVITIES

Gennady D. Maltsev
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Information Security, phone: (951)368-83-19, e-mail: gendosmal725@gmail.ru

Sergey N. Novikov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Professor, Department of Information Security, phone: (913)923-72-34, e-mail: snovikov@ngs.ru

The article uses the works of domestic and foreign scientists in the field of information security, information system security, legislative acts and regulatory documents of the Russian Federation. The purpose of the study is to develop indicators for assessing the organization 's control of license re-

quirements and conditions in terms of monitoring activities. As the importance of information increases, so does the number of problems with her protection. Methods of information theft are being improved, and there are more and more new ways of obtaining it without authorization. Therefore, the problem of information security has become particularly relevant. The methods of protection must meet the requirements, have a license and certificates of the relevant authorities. When performing the work, the literature on the topic was studied: "Regulatory framework". The methods of analysis, generalization, comparison, and classification were used in the work. Development of indicators for evaluating the organization for monitoring license requirements in terms of monitoring activities.

Keywords: information, indicators, means of protection, security, monitoring, licensing, requirements, regulatory regulation

В настоящее время информация занимает ключевое место. Да и во все времена полная и точная информация существенно помогает ее пользователю и дает преимущества перед другими пользователями, не обладающими точной и достаточно полной информацией.

С ростом важности информации растет и количество проблем с ее защитой [3]. Совершенствуются методы хищения информации, появляются все более новые способы ее несанкционированного получения [4]. Поэтому проблема защиты информации прибрела особую актуальность [10]. Для этого разрабатываются все новые и новые способы защиты. Наибольшей популярностью пользуются технические средства защиты [5]. К ним предъявляется множество требований, как и к организациям, которые занимаются производством таких средств и мониторингом информационной безопасности. Они должны соответствовать требованиям, иметь лицензию и сертификаты соответствующих органов [1].

Объектом исследования является деятельность организаций по контролю лицензионных требований и их мониторингу [6].

Предметом исследования являются показатели для оценки организации по контролю лицензионных требований и условий в части деятельности по мониторингу.

Цель данной работы – разработать показатели для оценки организации по контролю лицензионных требований и условий в части деятельности по мониторингу.

К задачам, решаемым в работе, относятся:

– анализ научных методов защиты;

– исследование нормативных актов, регулирующих деятельность по контролю лицензионных требований;

– выбор методов защиты, соответствующих требованиям ФСТЭК и ФСБ;

– математическое моделирование методов защиты;

– разработка показателей для оценки организации;

– использование показателей для оценки организации.

Главную часть исследования составляют труды отечественных и зарубежных ученых в области защиты информации, безопасности информационных систем.

Нами была изучена литература по нормативно-правовой базе, использованы различные методы исследования, проведен анализ, обобщение, сравнение, классификация.

Научная новизна работы заключается в том, что разработаны показатели для оценки организации по контролю лицензионных требований в части деятельности по мониторингу.

Теоретическая значимость и прикладная ценность полученных результатов в том, что данные рекомендации могут использоваться при организации контроля лицензионных требований в части деятельности по мониторингу.

Методы и материалы

Для обнаружения уязвимостей был выбран сетевой сканер XSpider [2]. По возможностям он не уступает, известным сканерам безопасности.

Высокое качество работы XSpider обеспечивается за счет:

– интеллектуального подхода к распознаванию сервисов;

– многочисленных ноу-хау, использующихся при поиске уязвимостей;

– уникальной обработки RFC-сервисов всех стандартов с их полной идентификацией;

– анализатора структуры и метода интеллектуального распознавания уязвимостей веб-серверов;

– постоянного обновления встроенной базы уязвимостей.

Проведены сравнения средств защиты информации от несанкционированного доступа (СЗИ от НСД) по нескольким показателям:

а) обеспечение защищенности от угрозы;

б) стоимость внедрения.

Результаты сравнения приведены. В таблице используются такие обозначения, как «+» – обеспечивает; «–» не обеспечивает[10].

Сравнение представленных СЗИ от НСД

Угрозы	«Dallas Lock 8.0-K»	«Аккорд-Win64 K»	«SecretNet 7»
1	2	3	4
Несанкционированная загрузка штатной ОС и получение НСД к информационным ресурсам	+	+	+
Нарушение целостности программной среды СВТ и состава компонентов аппаратного обеспечения СВТ	+	+	+
Утечка информации через USB-накопители	+	+	+
Доступ внутренних нарушителей к информации на рабочих станциях пользователей	+	+	+
Заражение вирусами			
Несанкционированный доступ к ресурсам локальной сети	+		
Несанкционированный доступ к информации при передаче через открытую сеть Интернет	+		
Стоимость, руб.:	59300	42390	55295

Обсуждение

По результатам проведенного сравнения сделаны выводы:

– стоимость СЗИ от НСД «DallasLock 8.0-K» самая высокая;

– система защиты информации от НСД «DallasLock 8.0-K» обеспечивает защиту рабочих станций, сервера и каналов связи, потому что идет в комплекте с фирменным межсетевым экраном;

– остается угроза реализации заражения вирусами.

На основании того, что в комплекте с СЗИ от НСД «Dallas Lock 8.0-K» поставляется межсетевой экран, сделан выбор в пользу данного средства защиты информации [7] [8].

Для сравнения системы обнаружения вторжений выбраны решения по следующим критериям:

– предлагаемые решения имеют один или несколько сертификатов (ФСТЭК, МО, ФСБ);

– поставщик решения российский;

– межсетевые экраны поставляются в составе программно-аппаратного комплекса (ПАК).

Каждое устройство имеет ряд особенностей:

– устройство «РУБИКОН-К» позволяет закрыть сразу два типа требований приказов от 11.02.2012 № 17 и от 18.02.2013 № 21 ФСТЭК России: требования к сертифицированным МЭ и требования к наличию средств обнаружения вторжений (СОВ);

– Altell NEO имеет ряд дополнительных функции (веб и почтовый фильтры), обладает гораздо более высокой стоимостью.

В основе IDS/IPS в межсетевых экранах нового поколения ALTELL NEO, лежит открытая технология Suricata.

В отличие от IDS/IPS Snort, используемая нами система обладает рядом преимуществ:

– позволяет использовать GPU в режиме IDS;

– обладает более продвинутой системой IPS;

– поддерживает многозадачность;

– обеспечивает более высокую производительность;

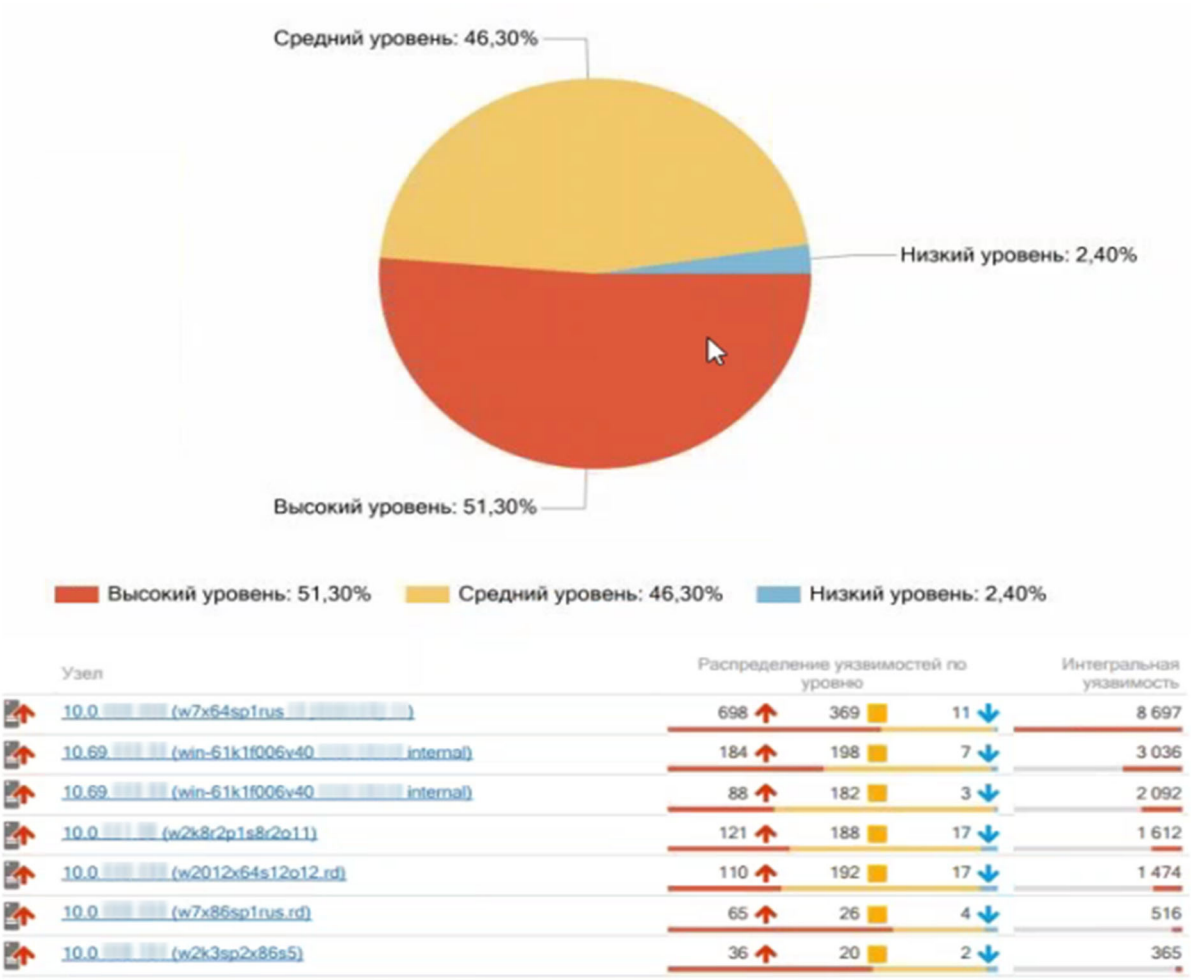
– полностью поддерживает формат правил Snort.

Заключение

По результатам сравнения SIEM (Security information and event management), можно сделать вывод, что для крупных организаций рекомендуется использовать решения от HP и IBM. Для организаций меньшего масштаба, рекомендуется рассмотреть решения от российских компаний Positive Technologies и ООО «ИТБ». Это выгодное решение для организаций, не готовых заниматься тонкой настройкой системы и которым не требуется специфичная гибкость платформы

для реализации главных функций SOC (Security Operations Center)[9]. SOC (Security Operations Center) – это команда ИБ специалистов ответственная за мониторинг безопасности и реагирования на инциденты.

В результате для расследования инцидентов была выбрана система MaxPatrol. На рисунке представлен отчет по возможным инцидентам, выявленным данной программой [10].



Узел	Распределение уязвимостей по уровню			Интегральная уязвимость
10.0 (w7x64sp1rus)	698	369	11	8 697
10.69 (win-61k1f006v40 internal)	184	198	7	3 036
10.69 (win-61k1f006v40 internal)	88	182	3	2 092
10.0 (w2k8r2p1s8r2o11)	121	188	17	1 612
10.0 (w2012x64s12o12.rd)	110	192	17	1 474
10.0 (w7x86sp1rus.rd)	65	26	4	516
10.0 (w2k3sp2x86s5)	36	20	2	365

Пример отчета по уязвимым узлам сети MaxPatrol

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).

2. ГОСТ Р 50922-96 Защита информации. Основные термины и определения.

3. Конституция Российской Федерации. Принята Всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // Российская газета. – 1993. – 25 декабря; Собрание законодательства РФ, 04.08.2014, N 31, ст. 4398.

4. Уголовный кодекс РФ (УК РФ) от 13.06.1996 N 63-ФЗ (ред. от 25.04.2018 N 17-П) // Собрание законодательства РФ. – 31.12.2012. — Доступ из СПС «КонсультантПлюс».

5. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. N 149-ФЗ (ред. от 08.06.2020 N 177-ФЗ) // Собрание законодательства РФ. – 31.12.2012. — Доступ из СПС «КонсультантПлюс».

6. О лицензировании отдельных видов деятельности: Федеральный закон от 04.05.2011 N 99-ФЗ (ред. 31.07.2020 N 270-ФЗ).

7. Об электронной подписи: Федеральный закон от 07 апреля 2011 г. (ред. 08.06.2020 N 181-ФЗ) // Собрание законодательства РФ. – 31.12.2012. — Доступ из СПС «КонсультантПлюс».

8. О персональных данных: Федеральный закон 152-ФЗ от 25.07.2011г. (ред. 24.04.2020 N 123-ФЗ) // Собрание законодательства РФ. – 31.12.2012. — Доступ из СПС «КонсультантПлюс».

9. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

10. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».