УДК 004.01
DOI 10.33764/2618-981X-2022-6-157-165

Критерии выбора показателей оценки организации по контролю лицензионных требований и условий в части деятельности по мониторингу систем информационной безопасности

Г. Д. Мальцев[1], С. Н. Новиков[1,2]*

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация

[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация

*e-mail: gendosmal725@gmail.com

Аннотация. С увеличением значимости информации увеличиваются проблемы с ее эффективной защитой. Способы защиты должны быть согласованы с соответствующими органами и иметь соответствующую документацию. Цель исследования – разработать критерии выбора показателей по контролю лицензионных требований и условий в части деятельности по мониторингу (систем) информационной безопасности. Для выполнения работы применялись следующие методы: метод анализа, обобщения, сравнения, классификации. Решения от российских компаний Positive Technologies и ООО «Инновации технологии безопасность», которые подойдут для малых предприятий. Была проведена оценка организации по кадрам и по средствам защиты. Разработаны критерии для выбора показателей оценки организации. Благодаря данным показателям можно легко определить, соответствует организация требованиям или нет, определить направления для доработки и защиты предприятия.

Ключевые слова: защита информации, оборудование, способы хищения информации, мониторинг, лицензирование, нормативное регулирование

Criteria for the selection of evaluation indicators of the organization for the control of licensing requirements and conditions in terms of monitoring information security systems

G. D. Maltsev[1], S. N. Novikov[2]*

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation

*e-mail: gendosmal725@gmail.com

Abstract. With the increasing importance of information, the problems with its effective protection increase. The methods of protection must be agreed with the relevant authorities and have the appropriate documentation.The purpose of the work is develop criteria for the selection of evaluation indicators of the organization for the control of licensing requirements and conditions in terms of monitoring information security systems.The following methods were used to perform the work: the method of analysis, generalization, comparison, classification. Solutions from Russian companies Positive Technologies and the Limited Liability Company "Innovation Technologies security", which are suitable for small businesses. The organization was evaluated by personnel and by means of protection. Criteria have been developed for the selection of organization evaluation indicators. Thanks to these indicators, it is easy to determine whether the organization meets the requirements or not, to determine the directions for improvement and protection of the enterprise.

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

Введение

Безопасность информационных систем основывается на защите от уязвимостей. Появление уязвимостей может возникать из-за ошибок в конфигурации компонентов информационной системы. Из-за этого система может быть атакована.

Объектом исследования является деятельность организаций по контролю лицензионных требований и их мониторингу [1]. Предметом исследования являются критерии выбора показателей для оценки организации по контролю лицензионных требований и условий в части деятельности по мониторингу.

Цель данной работы – определить критерии выбора показателей оценки организации по контролю лицензионных требований и условий в части деятельности по мониторингу.

К задачам, решаемым в работе, относятся:

- поиск известных методов защиты;
- исследование нормативно-правовой базы по контролю лицензионных требований;
- выбор методов защиты, соответствующих требованиям ФСТЭК (Федеральная служба по техническому и экспортному контролю) и ФСБ (Федеральная служба безопасности);
- разработка показателей для оценки организации;
- использование показателей для оценки организации.

Защита информации, безопасность информационных систем составляют основную часть исследования. Научная новизна работы заключается в том, что разработаны показатели для оценки организации по контролю лицензионных требований в части деятельности по мониторингу информационной безопасности.

Методы и материалы

Для поставленной задачи были рассмотрены самые современные и распространенные сканеры:

1. Net Recon;
2. XSpider;
3. Nmap;
4. Metasloit;
5. OpenVAS.

Они предназначены для реализации следующих задач:

1. Идентифицировать доступные сетевые ресурсы;
2. Идентифицировать доступные сетевые сервисы;
3. Идентифицировать уязвимости сетевых сервисов;
4. Выдавать рекомендации по устранению уязвимостей.

Сканеры уязвимостей сети при своей работе используют два основных механизма:

1. зондирование, не слишком оперативен, но точен. Это механизм активного анализа, который запускает имитации атак, тем самым проверяя уязвимость. При зондировании применяются методы реализации атак, которые помогают подтвердить наличие уязвимости и обнаружить ранее не выявленные «провалы»;

2. сканирование, более быстрый, но дает менее точные результаты. Это пассивный анализ, при котором сканер ищет уязвимость без подтверждения ее наличия, используя косвенные признаки. С помощью сканирования определяются открытые порты и собираются связанные с ними заголовки. Они в дальнейшем сравниваются с таблицей правил определения сетевых устройств, операционных систем и возможных «дыр». После сравнения сетевой сканер безопасности сообщает о наличии или отсутствии уязвимости.

Проведем сравнительный анализ выбранных программных средств.

Сравнивая и оценивая характеристики, выбираем интересующий нас вариант. Специальные сканеры нужны для нахождения специфического класса уязвимостей. Число уязвимостей в базах данных приближается к 1000.

Из наиболее современных сетевых сканеров можно выделить NetRecon компании Symantec в его базе находятся более 800 уязвимостей Windows, UNIX и NetWare. Обновления данной базы осуществляется через интернет.

NetRecon работает с сетевыми сервисами для нахождения уязвимостей,таких как ftp, telnet, DNS, электронная почта, Web-сервер и др.

Первым российским сканером безопасности является Сетевой сканер XSpider. XSpider проводит сетевой аудит для нахождения уязвимостей, и делает это удаленно.

Nmap («Network Mapper») проверяет сеть на безопасность используя открытый код.

Metasploit – средство для пинтеста и хакерства и т.п.

Metasploit Pro – это инструмент для проверки уязвимости и эксплуатации, который помогает разделить рабочий процесс тестирования на проникновение на более мелкие и более управляемые задачи.

OpenVAS – это сканер для нахождения уязвимостей, с его помощью можно управлять уязвимостями, у которых есть открытый код.

Для защиты каналов передачи данных используется программное обеспечение средство защиты информации от несанкционированного доступа (СЗИ от НСД). Проанализируем: СЗИ «Dallas Lock 8.0-K», «Аккорд-Win32 K/ Аккорд-Win64 K», «Secret Net 7». СЗИ «Dallas Lock 8.0-K» можно дополнить «Сервером безопасности». «Сервер безопасности Dallas Lock 8.0-K» контролирует все компьютеры в сети «Dallas Lock 8.0-K». Сеть под контролем указанного сервера «Dallas Lock 8.0-K», согласовывается с его клиентами и образуют домен безопасности «Dallas Lock 8.0-K». Рекомендуется использовать сервер «Dallas Lock 8.0-K» для 10 пользователей, а если пользователей больше 50 человек он обязателен для конфигурации [2]. СЗИ «Dallas Lock 8.0-K» – средство защиты информации от НСД для коммерческих организаций[3].

Стоимость внедрения приведена в табл. 1.

Таблица 1

Стоимость внедрения «DallasLock 8.0-K»

Название	Цена, руб.	Количество	Стоимость, руб.
«Dallas Lock 8.0-К» с модулем «Межсетевой экран» Право на использование (СЗИ НСД, СКН, МЭ).	8400	6	50400
«DallasLock 8.0» Сертифицированный комплект для установки	900	1	900
Идентификатор «Rutoken S (32 Кб)»	1250	6	7500
Итого			58800

ПАК (программно-аппаратный комплекс) СЗИ «Аккорд-Win32 К и Аккорд-Win64 К» компании ОКБ САПР предназначены для разграничения доступа к рабочим станциям [4].

Предусмотрена идентификация/аутентификация пользователя с помощью ТМ-идентификаторов DS 199x, устройств ШИПКА или смарт-карт. ПАК СЗИ работает на рабочих станциях.

Сумма установки в нашем случае приведена в табл. 2.

Таблица 2

Стоимость внедрения «Аккорд-Win32 K/Аккорд-Win64 K»

Название	Цена, руб.	Количество	Стоимость, руб.
ПАК «Аккорд-Win64 K»	5865	6	35190
Считыватель DS-USB TE (с фиксатором ТМ) на USB-порт	600	6	3600
Идентификатор ТМ DS 1993	600	6	3600
Итого			42390

СЗИ от НСД, имеющее сертификат MS Windows.

«SecretNet» – сертифицированное средство, которое подходит к требованиям о защите персональных данных, о коммерческой тайне, о государственной тайне и с требованиями стандарта Банка России [5].

Стоимость внедрения в нашем случае приведена в табл. 3.

Таблица 3

Стоимость внедрения Secret Net 7

Название	Цена, руб.	Количество	Стоимость, руб.
Право на использование Средства защиты информации SecretNet 7. Клиент (сетевой режим работы). Inc. TS Basiclvl	7920	6	47520
Установочный комплект. Средство защиты информации SecretNet 7 (сетевой).	275	1	275
Идентификатор Rutoken S (32 Кб)	1250	6	7500
Итого			55295

Общее название программ IDS (Intrusion Detection System - системы обнаружения вторжений).

Функциональные задачи SIEM

Задачами SIEM являются:

– система собирает данные и регистрирует все события

– может создавать отчет о всех действиях и в определенный период сообщает службе ИБ (информационная безопасность) [6].

Для выбора системы Security information and event managerment (SIEM – управление информацией о безопасности и управление событиями безопасности) сравним наиболее широко применяемые в Российской Федерации системы. Проведем сравнительный анализ систем расследования инцидентов. В табл. 4 приведено сравнение систем расследования инцидентов по наиболее важным критериям [7].

Таблица 4

Сравнение систем расследования инцидентов

Критерий	IBM Qradar	Security Capsule	HP ArcSight	MaxPatrol SIEM
› Наличие в реестре российских программ для электронных вычислительных машин и баз данных Минкомсвязи России	–	Да	–	Да
› Работа с источниками АСУ ТП	Частично	Да	Да	Частично
› Принцип работы	Снифер	Syslog, Eventlog, SNMP, SQL, собственный протокол	Сбор и последующий анализ логов (в том числе по Syslog и с сетевых устройств)	С помощью протокола удалённого доступа происходит подключение к системе, аутентификация, авторизация, сбор логов. На данный момент SIEM Maxpatrol работает в большинстве своем только в связке с системой контроля защищенности и соответствия стандартам Maxpatrol.
› Цена	от 3 млн. руб.	от 200 тыс. руб.	от 4 млн. руб.	от 3 млн. руб.

Далее нужно выбрать средства защиты, соответствующие требованиям ФСТЭК России.

Выбор методов защиты, соответствующих требованиям ФСТЭК России и ФСБ

Чтобы обнаружить уязвимости подойдет сетевой сканер XSpider. Он не уступает известным сканерам, а в некоторых деталях даже справляется лучше [8].

XSpider проводит свою работу качественно за счет:

– аналитического метода к определению сервисов;

– множества оригинальных способов для нахождения уязвимостей;

– редкого производства RFC-сервисов всех стандартов с их полной идентификацией;

– анализатора структуры и метода разумной идентификации уязвимостей веб-серверов;

– постоянного обновления базы уязвимостей.

Проведем сравнительный анализ характеристик, выбранных СЗИ от НСД. Сравнение СЗИ от НСД разобьём на два параметра: цена и защищенность. Данные указаны в табл. 5.

Таблица 5

Сравнение представленных СЗИ от НСД

Угрозы	«Dallas Lock 8.0-K»	«Аккорд-Win64 K»	«SecretNet 7»
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

В результате сравнения делаем выводы:

– СЗИ от НСД «DallasLock 8.0-K» существенно дороже аналогичных систем, зато защитит несколько каналов передачи данных, потому что предоставляется в комплекте с межсетевым экраном [9];

– останется только защититься от заражения вирусами.

Останавливаем выбор на СЗИ от НСД «Dallas Lock 8.0-K».

Сравнение систем начинается с выбора критериев:

– предлагаемые решения имеют один или несколько сертификатов (ФСТЭК России, МО, ФСБ) [10];

– поставщик – российский;

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

Для выявления инцидентов была выбрана система MaxPatrol.

Показатели для оценки организации по контролю лицензионных требований и условий в части деятельности по мониторингу вытекают из требований к организациям, претендующим на лицензию по мониторингу ИБ.

Показатели можно сгруппировать по следующим критериям:

– персонал;

– рабочие площади;

– оборудование;

– документация;

– СЗИ.

Для оценки организации можно использовать балльную систему согласно таб. 6, 7.

Таблица 6

Оценка организации по кадрам

Должность	Образование	Стаж	Количество баллов
Директор	Высшее образование в сфере ИБ	до 1 года 1-3 года 3-5 лет свыше 5 лет	0 0 1 2
	Высшее образование в сфере технических наук	до 1 года 1-3 года 3-5 лет свыше 5 лет	0 0 0 1
	Любое высшее образование+аттестат о переподготовке	до 1 года 1-3 года 3-5 лет свыше 5 лет	0 0 0 1
Специалист (количество баллов умножается на количество специалистов)	Высшее образование в сфере ИБ	до 1 года 1-3 года 3-5 лет свыше 5 лет	0 0 1 2
	Любое высшее образование+аттестат о переподготовке	до 1 года 1-3 года 3-5 лет свыше 5 лет	0 0 1 2
Итого минимальное требуемое количество баллов			7-8

Таблица 7

Оценка организации по наличию СЗИ

Оборудование и СЗИ	Выполняемые функции	Количество баллов
Межсетевой экран уровня веб-сервера	Контроль и фильтрация в соответствии с заданными правилами информационных потоков по протоколу передачи гипертекста, проходящих через него Сертификат ФСТЭК России Не ниже чем по 4 классу защиты	1 1 1
Межсетевой экран уровня сети	Контроль и фильтрация в соответствии с заданными правилами информационных потоков, проходящих через него. Применяется на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы Должен иметь сертификат ФСТЭК России Не ниже чем по 4 классу защиты	1 1 1
Средство (средства) антивирусной защиты	Должно иметь сертификат (сертификаты) ФСТЭК России Не ниже чем по 4 классу защиты	1 1

За соответствие помещения, оборудования и документации можно насчитать по одному баллу.

В табл. 6, 7 представлена бальная оценка выбора по стажу, применяемая к высшему руководству и специалистам, для соответствия требованиям по контролю лицензионных требований и условий в части деятельности по мониторингу.

Таким образом, для соответствия организации требованиям лицензионного контроля в части деятельности по мониторингу необходимо набрать 29-30 баллов.

Заключение

В результате сравнительного анализа были выбраны следующие программные средства: сетевой сканер XSpider, СЗИ от НСД «DallasLock 8.0-K», MaxPatrol.

Разработаны критерии для выбора показателей оценки организации. Основными критериями являются: требования к персоналу, помещениям, наличию технических средств защиты, наличию документации, наличие соответствующего программного обеспечения [11].

Благодаря данным показателям можно легко определить, соответствует организация требованиям или нет, определить направления для доработки и защиты предприятия. Потому что защита информации – это важная составляющая в современном постоянно развивающемся обществе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ (ред. от 08.06.2020 № 177-ФЗ) // Собрание законодательства РФ. – 31.12.2012. — Доступ из СПС «КонсультантПлюс»/

3. Москвитин, Г.И. Комплексная защита информации в организации / Г.И. Москвитин. - М.: Русайнс, 2017. - 400 с.

4. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, 2018. - 176 с.

5. Дурнев Р.А. Безопасность России. Основы информационно-психологической безопасности / Р.А. Дурнев. - М.: Знание, 2019. - 616 с.

6. Чипига А. Ф. Информационная безопасность автоматизированных систем / А. Ф. Чипига. – М.: Гелиос АРВ, 2010. – 336с.

7. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

8. ГОСТ Р ИСО/МЭК 27007-2014 Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности [Текст]: нац. стандарт РФ. – Введ. 01.06.2015. – Стандартинформ, 2019. – 28 с.

9. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

10. Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»

11. Герасименко В. А., Малюк А. А. Организация комплексной защиты информации на современных объектах / В.А Герасименко-М. : Кн.мир, 2011. – 103 с.