УДК 004.054.53
DOI: 10.33764/2618-981X-2020-6-1-99-103

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ ОБОРОННО-ПРОМЫШЛЕННОГО КОМПЛЕКСА

Анастасия Сергеевна Голдобина
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры информационной безопасности; тел. (923)220-80-89, e-mail: nastya-gold09@mail.ru

Юлия Алексеевна Исаева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры информационной безопасности; тел. (913)980-23-09, e-mail: isaeva.ja@hotmail.com

Дмитрий Михайлович Никулин
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент кафедры фотоники и приборостроения, тел. (383)344-29-29, e-mail: dimflint@mail.ru

Компоненты защиты информационной системы управления производством оборонно-промышленного комплекса представляют собой единый механизм, способный защищать информацию ограниченного доступа от возможных нарушителей. Если один из элементов защиты информации будет работать неэффективно, то это станет проблемой для всей системы защиты оборонно-промышленного комплекса. Информационным системам управления производством необходимо учитывать все доступные способы предотвращения утечки информации, для этого собственники оборонно-промышленных комплексов должны проводить оценку эффективности. В статье предложен возможный путь решения проблемы при рассмотрении одной из важнейших подсистем: система обнаружения вторжений. В настоящий момент не разработана методика проведения оценки эффективности системы обнаружения вторжений для информационных систем управления производством. Настоящая система расположена на реальном объекте, расположенном в Иркутской области и принадлежащем к оборонно-промышленному комплексу.

Ключевые слова: оценка эффективности, информационная система управления производством, система защиты информации, система обнаружения вторжений.

EVALUATION OF THE EFFICIENCY OF INTRUSION DETECTION SYSTEMS IN PRODUCTION MANAGEMENT INFORMATION SYSTEM OF A MILITARY-INDUSTRIAL COMPLEX

Anastasiya S. Goldobina
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (923)220-80-89, e-mail: nastya-gold09@mail.ru

Julia A. Isaeva
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (913)980-23-09, e-mail: isaeva.ja@hotmail.com

Dmitry M. Nikulin
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Department of Photonics and Device Engineering, phone: (383)344-29-29, e-mail: dimflint@mail.ru

Security components of the production management information system of the military-industrial complex are a single mechanism that can protect restricted access information from possible violators. If one of the elements of information security does not work efficiency, it will become a problem for the entire defense system of the military-industrial complex. Production management information systems need to take into account all available ways to prevent information leakage to do this, the owners of military-industrial complexes must conduct an efficiency assessment. The article suggests a possible way to solve the problem when considering one of the most important subsystems: intrusion detection system. Currently, there is no methodology for evaluating the efficiency of intrusion detection systems for production management information systems. This system is located on a real object located in the Irkutsk Region and belongs to the military-industrial complex.

Key words: efficiency evaluation, production management information system, information security system, intrusion detection system.

Введение

В настоящий момент Российская Федерация стоит на этапе взрывного технологического роста оборонно-промышленных комплексов (далее – ОПК), вызванного четвёртой технологической революцией, которая повлекла за собой необходимость защиты от внешних угроз со стороны различных типов нарушителей. Одним из главных процессов, защищаемых в ОПК стали информационные системы управления производством (далее – ИСУП), которые содержат в себе информацию с грифом секретности и требуют постоянной защиты. В [3] устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обработка которой осуществляется в ИСУП ОПК, от несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях её добывания, уничтожения, искажения или блокирования доступа к ней.

Компоненты защищённой инфраструктуры ИСУП ОПК представляют собой единый механизм, способный защищать конфиденциальную информацию. Если один из элементов системы защиты будет работать неэффективно, то это станет проблемой для всего механизма защиты информации.

Методы и методики

Согласно [2], перед вводом в эксплуатацию должны проводиться предварительные испытания, включая проверку работоспособности всей подсистемы безопасности и отдельных средств защиты информации.

Для того, чтобы обеспечить информационную безопасность на предприятиях ОПК и, при этом избежать вторжения внешних нарушителей в ИСУП, необходимо правильно проводить оценку эффективности системы защиты информации в ОПК. Анализ требований [2] показал, что оценка эффективности может проводиться в форме повторной аттестации.

В случае, когда требований к оценке эффективности нет, а также на объекте уже внедрены средства защиты информации, субъекту необходимо проводить оценку эффективности самостоятельно на различных этапах стадии внедрения организационных и технических мер по обеспечению безопасности.

Для исследования был выбран один из важнейших компонентов системы защиты информации – система обнаружения вторжений (далее – СОВ).

В настоящий момент не существует методик оценки эффективности СОВ для ИСУП ОПК по причине того, что данный класс средств оценить довольно трудно. Для оценки эффективности необходимо смоделировать ситуации, в которых СОВ покажет на практике свой функционал, а также векторы угроз.

Оценка эффективности СОВ должна соответствовать целям защиты. Вероятно, для разработки методики можно воспользоваться существующей системой требований на базе стандартов ИСО/МЭК 15408 [5], [6], [7], активно используемой ФСТЭК России.

При использовании «Общих критериев» [5], [6], [7] объект оценки, которым в данном случае будет являться СОВ, рассматривается не сам по себе, а в контексте окружающей его среды функционирования. Во время подготовки к оценке эффективности должны быть выделены требования к окружающей среде, именуемые в дальнейшем - аспекты среды функционирования СОВ. Аспекты среды функционирования СОВ содержат в себе следующие компоненты:

– предположения безопасности содержит различные концепции безопасности среды, в которой будет использоваться СОВ или предполагается к использованию;

– угрозы безопасности, включающие все угрозы безопасности информации, для которых требуется защита средствами СОВ или окружающей его среды;

– политики безопасности, идентифицирующие и, при необходимости, объясняющие все положения политики безопасности организации или правила, которым должна подчиняться СОВ.

Для оценивания аспектов среды функционирования системы обнаружения вторжений был использован функционал СОВ: фабрика безопасности Fortinet.

Для достижения поставленных целей к фабрике безопасности Fortinet предъявляются требования безопасности. Согласно [4], в отношении фабрики безопасности Fortinet должны быть проведены испытания, предусматривающие:

1) тестирование средства;

2) испытания по выявлению уязвимостей и недекларированных возможностей средства;

3) проведение анализа скрытых каналов в средстве.

Тестирование и анализ скрытых каналов проводятся только для средств защиты информации.

ГОСТ Р ИСО/МЭК 18045-2013 [8] предъявляет две группы требований – это требования безопасности, предъявляемые к функциям безопасности объекта оценки, и требования доверия, предъявляемые к технологии и процессу разработки, эксплуатации и оценки объекта и призваны гарантировать адекватность реализации механизмов безопасности.

Разработка оценки эффективности Fortinet в ИСУП ОПК необходима для обеспечения информационной безопасности всех векторов от возможных атак.

Результаты

Информационная система, на которой будут проведены испытания представляет собой комплекс территориально распределённых объектов АСУ ТП на территории Иркутской области. Физическое подключение объектов АСУ ТП к обследуемой системе ИСУП реализовано через коммутатор. Все межкоммутаторные соединения организуются на уровне L2 модели взаимодействия OSI.

В имитационной модели для оценивания показателя эффективности управления ИСУП ОПК используется следующая мультипликативная форма:

$$W_э = P_{св.сб} \cdot P_{пр} \cdot P_{св.пр} \cdot P_p \quad (1)$$

где $P_{св.сб}$ – вероятность своевременного сбора всей необходимой для принятия решений информации;

$P_{пр}$ – вероятность правильного принятия решений;

$P_{св.\ пр}$ – вероятность своевременного и правильного принятия решений;

$P_{св.\ р}$ – вероятность своевременной реализации принятых решений.

Показатель эффективности управления техническими средствами $W_э$, обеспечиваемый средствами управления с рассматриваемым вариантом состава ее построения и принятым алгоритмом управления, определяется с помощью формулы (1).

На основе мультипликативной формулы (1) высчитывались показатели оценки эффективности и были получены следующие результаты:

– время цикла управления 11,558 секунд;

– время ожидания обработки 12,484 секунд;

– $P_{св.\ инф} = 0{,}868$;

– $P_{пр} = 0{,}868$;

– $P_{св\ пр} = 0{,}118$;

– $W_э = 0{,}088$.

Заключение

В результате проведения оценки эффективности будет разработано заключение, подтверждающее, что информационная система соответствует актуальным требованиям ФСТЭК России, в том числе подтверждает:

– эффективность работы фабрики безопасности fortinet;

– отсутствие возможных уязвимостей в системе;

– выявление потенциальных внутренних нарушителей безопасности информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/42128, свободный (дата обращения: 10.03.2019).

2. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». [Электронный ресурс]. Режим доступа: https://minjust.consultant.ru/documents/38914, свободный (дата обращения: 10.03.2019).

3. Приказ ФСТЭК России от 28 февраля 2017 г. № 31 ДСП «Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых организациями оборонно-промышленного комплекса».

4. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)» - Утверждены Приказом ФСТЭК России от 30 июля 2018 г. №131.

5. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200101777, свободный (дата обращения: 10.03.2019).

6. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200105710, свободный (дата обращения: 10.03.2019).

7. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200105711, свободный (дата обращения: 10.03.2019).

8. ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200105309, свободный (дата обращения: 10.03.2019).

9. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под.ред. А.С.Маркова. Москва: Радио и связь, 2012. 192 с.