IPTV Middleware – проміжне програмне забезпечення для управління комплексом IPTV. Це основний компонент IPTV рішення, оскільки він, в підсумку, і визначає набір послуг, доступний абоненту, користувацький інтерфейс, логіку переходів і алгоритм управління. На Middleware покладається роль координатора в процесі взаємодії практично усіх компонентів комплексу.

Ядро підсистеми управляє зовнішніми компонентами комплексу, підтримує базу даних абонентів та наданих їм послуг, займається аутентифікацією та авторизацією абонентських пристроїв, взаємодіє із системою обліку послуг (система управління майном, в готелі — система прийому-поселення) [4].

Абонентський портал (інша назва: Інтерфейс абонента, Subscriber User Interface, SUI) — «Обличчя» всього комплексу, інтерфейс, який бачить абонент на своєму екрані, і завдяки якому він користується послугами.

Список використаних джерел

1 Технологія IPTV [Електронний ресурс] Режим доступу: http://iptv.at.ua/ - Назва з екрану. Дата звернення: 22.09.2015

2 IPTV – [Електронний ресурс] Режим доступу: https://ru.wikipedia.org/wiki/IPTV - Назва з екрану. Дата звернення: 17.09.2015

3 Размышления об IPTV С.Мориц.– [Електронний ресурс] Режим доступу: http://www.lastmile.su/journal/article/2095/. Дата звернення : 22.09.2015.

4 Архитектура IPTV - [Електронний ресурс] Режим доступу: https:// //www.iconsult.com.ua/index.php?id=275/ - Назва з екрану. Дата звернення: 22.09.2015.

УДК 004.94

ИСПОЛЬЗОВАНИЕ ПРИНЦИПОВ CYBER DEFENSE SITUATIONAL AWARENESS ДЛЯ ВЫЯВЛЕНИЯ НАРУШЕНИЙ ПРИ ВЫПОЛНЕНИИ СЕЛЬСКОХОЗЯЙСТВЕННЫХ РАБОТ

И. В. Михайлюк

Черниговский национальный технологический университет
ул. Шевченко, 95, г. Чернигов, Украина 14027, cstu@stu.cn.ua

Современное сельхозпредприятие представляет собой сложную распределенную систему, в состав которой входят множество разнородных объектов управления, функционирование которых направлено на выращивание с.-х. продукции. На эффективность выполнения работ оказывают сильное воздействие внешние факторы (погодные условия, влияние социальной среды, и т.д.) [1].

Для оперативного управления с.-х. работами необходимо учитывать множество факторов, влияющих на процесс выполнения и качество работ. Помимо этого необходимо выявлять нарушения, которые возникают по вине персонала. Эти нарушения можно расценивать как атаку на процесс

выполнения с.-х. операцию.

Термин атака в IT-технологиях употребляется в области защиты информации. Применительно к с.-х. технологиям его можно понимать как целенаправленное вмешательство в процесс реализации с.-х. операций, приводящее к отклонению последнего от регламента, предписанного технологическими картами, с целью не связанной с нуждами производства.

Используя аналогию кибератаки и атаки на с.-х. операцию, для выявления последней необходимо учитывать такие аспекты:

1. Осведомленность события. Идентификация ситуации, также может включать в себя идентификацию типа атаки, источник нападения, цель нападения[2].

2. Осведомленность о влиянии атаки. Оценка текущего воздействия (оценка ущерба) и оценка будущего воздействия.

3. Отслеживание развития ситуации (situation tracking).

4. Актеры атаки. Аспект ориентирован на поведение актера и его действия, а не на развитие ситуации в целом.

5 Аспект причинности, какое событие, чем вызвано (back-tracking).

6. Качество собранной информации (правдивость, полнота, и актуальность);

7. Аспект прогнозирования. Оценка возможных вариантов будущего развития текущей ситуации.

Кибер осведомленность ситуации (cyber situation awareness) может рассматриваться как трехфазный процесс: выявление ситуации (в том числе аспекты 1, 6 и 7), понимание ситуации (в том числе аспекты 2, 4 и 5), и проекция ситуации (в том числе аспект 3).

Целями киберзащиты есть идентификация эффективных планов реагирования и принятие оптимальных решений по конкретной атаке.

Актуальным есть вопрос сбора первичной информации, что в условиях распределенного с.-х. предприятия, ставит задачу разработки устройств сбора, передачи и первичной обработки информации.

Литература

1 Lytvynov V.V. Functional features of dispatching control centre for automatic control system of agricultural enterprise / V.V. Lytvynov, I. V. Mykhailiuk, A. S. Posadska // Математичні машини і системи. – 2014. – №3. – С. 67-77.

2 Barford P. Cyber SA: Situational Awareness for Cyber Defense / P. Barford, M. Dacier, T. G. Dietterich // – Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.173.6434&rep=rep1&type=pdf – Назва з екрана.