А. Г. Дупленко
ФГАОУ ВО «Балтийский федеральный университет имени Иммануила Канта»
236041 Калининград, ул. А. Невского, 14
duplenko@list.ru

Анализ состава угроз для информационной безопасности в высокоорганизованных системах типа «Умный город»

Одной из тенденций развития человеческого общества в последние десятилетия является стремительный рост городского населения. По некоторым оценкам, прирост населения городов в мире в совокупности за последние десять лет составил около 40 процентов [1, с. 10].

Значительный прирост городского населения имеет целый ряд негативных последствий, одним из наиболее опасных среди которых является повышенная нагрузка на службы, обеспечивающие функционирование городской инфраструктуры. Во многих странах наблюдается значительное отставание технических и технологических характеристик всех инфраструктурных служб от требований, которые предъявляет все более интенсивное их использование. Не являются исключением и российские города.

Одновременно в мире все более активно развиваются технологии, позволяющие добиваться эффекта «умного» дома, района или даже города. Данные высокоорганизованные системы так и называют – «Умный дом», «Умный город» и т.п. Их задачей является повышение эффективности систем энерго-, водо- и теплоснабжения, водоотведения и пр., обеспечение безопасности и комфорта. К настоящему времени в мире насчитывается, по некоторым оценкам, около 140 проектов «Умного города» разной степени завершенности Большинство из данных проектов сконцентрированы в Северной Америке и Западной Европе [2].

Поскольку высокоорганизованные системы типа «Умный город» связаны с объектами жизнеобеспечения населения, из умышленные либо неумышленные сбои и повреждения могут представлять серьезную угрозу. Этим объясняется высокий интерес к исследованиям по обеспечению информационной безопасности данных систем.

Под угрозами информационной безопасности многие специалисты понимают потенциальную возможность нарушения доступности, целостности и конфиденциальности информации. При этом угроза может быть реализована исполнителем, процессом или стихией [3, с. 3]. Применительно к системе «Умный город» самую большую опасность представляет несанкционированный доступ вследствие нарушения ее доступности, результатом чего могут быть сбои функционирования с последующим выводом из строя систем жизнеобеспечения.

Состав угроз для информационной безопасности в высокоорганизованных системах типа «Умный город» мы бы предложили классифицировать по их потенциальным носителям (разработчики информационного обеспечения, обслуживающий персонал, пользователи и злоумышленники), а также по направлениям угрозы - угрозы сбоя функционирования системы вследствие программных ошибок, внешних проблем с оборудованием, проблем с данными и нарушения информационного обмена. В общем виде из можно соотнести следующим образом (таблица 1):

Таблица1

Состав угроз для информационной безопасности в высокоорганизованных системах типа «Умный город»

Причина угрозы сбоя системы	*Разработчики ПО*	*Обслуживающий персонал*	*Пользователи*	*Злоумышленники*
Программные ошибки	+			
Проблемы с оборудованием		+++	+	+++
Проблемы с данными		++++	+	++
Информационный обмен	+	++	+	+++

Потенциальными носителями угрозы сбоя функционирования системы «Умный город» вследствие ошибок в программном обеспечении являются его разработчики.

К угрозам сбоя функционирования системы вследствие внешних проблем с оборудованием можно отнести хищение оборудования обслуживающим персоналом или злоумышленниками; неумышленный или умышленный вывод из строя (уничтожение) оборудования, а также носителей данных.

К угрозам сбоя функционирования системы вследствие проблем с данными относятся порча данных, их модификация при разрешенном доступе (обслуживающий персонал) как умышленные, так и неумышленные, ошибки ввода, искажение данных и ввод ложной информации при несанкционированном доступе и т.п.

К угрозам сбоя функционирования системы вследствие нарушения информационного обмена можно отнести блокирование (установка помех, закладок) ТС, каналов связи, проходов, задержку передачи информации (замедление, выставление доп. требований, пауза…); выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий обслуживающего персонала, пользователей, злоумышленников (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.).

Соответственно, в качестве направлений снижения угроз информационной безопасности в высокоорганизованных системах типа «Умный город» можно предложить следующие.

Во-первых, анализ и тестирование предлагаемого к использованию программного обеспечения с целью проверки обеспечения защиты от специфических угроз для систем подобного типа.

Во-вторых, обеспечение контроля за действиями обслуживающего персонала систем «Умный город», который должен включать разделение режимов доступа, сохранение информации о произведенных операциях, введенных, скаченных и переданных данных, автоматическую блокировку команд, которые создают опасность сбоя функционирования отдельного оборудования или всей системы и т.д.

В-третьих, обеспечение контроля за действиями пользователей системы «Умный город» с целью предотвращения возможных проблем с функционированием оборудования, данными и информационным обменом.

В-четвертых, предотвращение несанкционированного доступа к оборудованию, базам данных, каналам связи системы «Умный город», что должно включать в себя целый комплекс мер. Одним из важнейших направлений при этом являются криптографические методы защиты информации.

Литература

1. Владимирова Т.А., Соколов В.Г., Соколов С.А. Надежность функционирования и развития экономических систем с высоким технологическим укладом // Сибирская финансовая школа. 2015. – №6 (113). – С. 7 – 12.

2. Дрожжинова В.А. Умные города: потенциал и перспективы развития в регионах России // Сайт НИУ «Высшая школа экономики». 2016. URL: https://irsup.hse.ru/news/120291071.html (дата обращения: 21.11.2016).

3. Курчеева Г.И., Денисов В.В. Угрозы для информационной безопасности в высокоорганизованных системах типа «Умный город» // Интернет-журнал «Науковедение» Том 8, №3 (2016). URL: http://naukovedenie.ru/PDF/146EVN316.pdf (дата обращения: 11.10.2016).