УДК 004.056

МИЛУШЕВ ЭДУАРД ХАНИФОВИЧ,
кандидат технических наук, доцент,
Воронежский государственный технический университет.
ВОЛОДКИН ДМИТРИЙ АЛЕКСАНДРОВИЧ,
ассистент,
Воронежский государственный технический университет.
ЧАРЫКОВ ДАНИИЛ СЕРГЕВИЧ,
студент,
Воронежский государственный технический университет.
КАЛЯГИН ПЁТР ОЛЕГОВИЧ,
студент,
Воронежский государственный технический университет.

БЕЗОПАСНОСТЬ ЖИЛИЩА: ОТ ПОЖАРНОЙ СИГНАЛИЗАЦИИ ДО ЗАЩИТЫ ОТ КИБЕРУГРОЗ

Понятие «безопасность жилища» сегодня кардинально изменилось. Если всего пару десятилетий назад оно ассоциировалось с надежным замком на двери и исправной электропроводкой, то теперь наш дом превратился в сложный гибрид физического и цифрового пространства. Традиционные угрозы, такие как пожар или кража со взломом, никуда не исчезли, но к ним добавились новые, невидимые и оттого не менее опасные — киберугрозы. Умные колонки, подключенные к интернету камеры, интеллектуальные термостаты и бытовая техника — все эти устройства создают комфорт, но одновременно открывают новые «окна», через которые в нашу личную жизнь могут проникнуть злоумышленники.

The concept of "home security" has changed dramatically in recent years. While a few decades ago it was associated with a secure door lock and well-maintained electrical wiring, our homes have now become a complex hybrid of physical and

digital spaces. While traditional threats such as fire or burglary remain, they have been joined by new and invisible cyber threats. Smart speakers, internet-connected cameras, smart thermostats, and household appliances all create comfort, but they also open new "windows" through which intruders can enter our personal lives.

Ключевые слова: *безопасность жилища, пожарная сигнализация, киберугрозы, умный дом, защита от проникновения, датчики утечки, Wi-Fi безопасность, экологическая безопасность, цифровая гигиена, слоеная защита, человеческий фактор, культура безопасности.*

Key words: *home security, fire alarm systems, cyber threats, smart homes, intrusion protection, leakage sensors, Wi-Fi security, environmental safety, digital hygiene, layered protection, human factor, and security culture.*

Пожарная безопасность: больше, чем огнетушитель

Защита от пожара была и остается краеугольным камнем безопасности жилища. Однако сегодня это не просто огнетушитель в углу и памятка о том, что утюг нужно выключать. Современные технологии превратили пассивную пожарную безопасность в активную интеллектуальную систему, способную предотвратить катастрофу или минимизировать ущерб от нее. Современные системы раннего обнаружения:

1. Автономные дымовые извещатели — это необходимый минимум, но теперь они эволюционировали. На смену приходят комбинированные датчики, реагирующие не только на дым, но и на резкий рост температуры, что позволяет точнее определить характер возгорания и снизить количество ложных срабатываний.

2. Датчики утечки газа становятся все более востребованными, особенно в квартирах с газовым оборудованием. Лучшие модели не только издают пронзительный звук, но и способны послать уведомление на ваш смартфон, а в составе системы «умный дом» — автоматически перекрыть подачу газа через специальный клапан.

3. Системы «умный дом» выводят пожарную безопасность на новый уровень. Они интегрируют разрозненные датчики в единую сеть. В случае срабатывания дымового извещателя такая система может:

а) отправить push-уведомление и SMS владельцу;

б) автоматически отключить электропитание в проблемной зоне (кроме цепей, питающих систему безопасности);

в) подсветить пути эвакуации;

г) самостоятельно оповестить службы МЧС через охранный пульт.

Профилактика: основа, которую не заменят никакие технологии:

Никакие умные гаджеты не отменяют необходимости соблюдать базовые правила:

1. Исправность электропроводки — главное правило. Регулярно проверяйте розетки, вилки и провода бытовых приборов на предмет повреждений, не допускайте перегрузки сетевых фильтров и розеток.

2. Правильная эксплуатация приборов. Не оставляйте без присмотра включенные обогреватели, плиты и зарядные устройства. Следите за тем, чтобы легковоспламеняющиеся предметы (шторы, полотенца) находились на безопасном расстоянии от источников тепла.

Защита от проникновения: от механического замка до умной камеры

Защита дома от несанкционированного проникновения прошла путь от простого запирания двери на ключ до сложных многоуровневых систем, где физическая прочность сочетается с цифровым интеллектом. Современный подход предполагает создание нескольких рубежей обороны, каждый из которых усложняет задачу для злоумышленника.

Эволюция физической защиты: фундамент безопасности

1. Надежные двери и окна: Основной барьер — это входная дверь. Современные стандарты рекомендуют металлические двери с терморазрывом, усиленными петлями и противосъемными ригелями. Не менее важны и окна: для нижних этажей имеет смысл установить стеклопакеты с противовзломной

фурнитурой, которая не позволяет открыть створку снаружи даже при разбитом стекле.

2. Современные типы замков: Механическая часть защиты по-прежнему критична. Эффективна установка двух и более замков разных типов:

а) сувальдные замки устойчивы к силовому взлому;

б) цилиндровые замки (особенно с защитой от высверливания и вырывания, например, формата «перфокарта») сложно вскрыть отмычкой. Ключевой принцип — создание времени, которое потребуется злоумышленнику на преодоление каждого рубежа.

Электронные системы: цифровые «сторожа». Физическую защиту дополняют и усиливают электронные системы, которые выполняют три ключевые функции: предупреждение, обнаружение и документирование.

1. Видеодомофоны и видеоглазки: позволяют идентифицировать гостя, не подходя к двери. Модели с возможностью записи и удаленным доступом со смартфона дают возможность видеть происходящее у вашей двери из любой точки мира.

2. Датчики открытия окон и дверей: Эти компактные устройства — основа системы сигнализации. При срабатывании они отправляют мгновенное уведомление на телефон владельца и, если система подключена к пульту охраны, вызывают группу быстрого реагирования.

3. IP-камеры с уведомлениями на смартфон: выполняют роль и средства сдерживания (видимая камера отпугнет большинство воров), и инструмента наблюдения. Современные камеры умеют отличать движение человека от движения животного или автомобиля, отправляя релевантные уведомления, а не «спам» от каждого пролетающего листа. Ночная съемка и детектор оставленных предметов расширяют их функционал.

Бытовые и экологические риски: невидимая угроза внутри дома

Пока мы опасаемся взломов и пожаров, внутри нашего жилища могут незаметно накапливаться угрозы иного рода — тихие, медленные, но оттого не

менее опасные. Речь идет о бытовых авариях и экологических факторах, которые подрывают не только целостность нашего имущества, но и здоровье.

Техногенные аварии: датчики как страховка от катастрофы

1. Утечка газа: Эта угроза по-прежнему смертельно опасна. Современные датчики утечки газа — это не просто звуковая сигнализация. Интегрированные в систему «умного дома», они способны автоматически перекрыть подачу газа через запорный клапан с электроприводом, отправить уведомление хозяину и запустить вытяжку для проветривания. Это превращает потенциальную катастрофу в управляемый инцидент.

2. Протечка воды: Одна из самых частых и финансово-емких бытовых проблем. Датчики протечки, установленные в местах потенциального прорыва (под раковиной, стиральной машиной, возле батарей), обнаруживают воду до того, как она зальет соседей. В связке с умными кранами они могут самостоятельно перекрыть воду во всей квартире, спасая от многомиллионных ремонтов.

Экологическая безопасность: чем мы дышим?

Воздух внутри квартиры часто в 2-5 раз грязнее уличного. Его основные «загрязнители» невидимы, но их влияние на здоровье — нет.

1. Плесень и грибок: Постоянная сырость, плохая вентиляция в ванной и на кухне приводят к их появлению. Споры плесени — сильнейший аллерген и токсин, провоцирующий респираторные заболевания, головные боли и снижение иммунитета.

2. Летучие органические соединения (ЛОС): они выделяются из мебели из ДСП, лаков, красок, дешевых отделочных материалов и даже бытовой химии. Длительное воздействие ЛОС может вызывать токсические эффекты.

3. Пыль и аллергены: Бытовая пыль, пылевые клещи, шерсть животных — постоянные спутники городской квартиры, виновники аллергий и астмы.

Как решить эти проблемы?

1. Датчики качества воздуха (например, сенсоры PM2.5/PM10 для пыли, CO_2, ЛОС) становятся все доступнее. Они дают объективную картину и показывают, когда необходимо проветривание.

2. Приточные клапаны и бризеры обеспечивают постоянный приток свежего, очищенного от уличной пыли и аллергенов воздуха без сквозняков и шума.

3. Очистители воздуха эффективно удаляют из воздуха взвешенные частицы, пыльцу и аллергены. Регулярная влажная уборка и контроль влажности (с помощью увлажнителей или осушителей) завершают картину здорового микроклимата.

«Умный дом» — умные ли угрозы?

Технологии «умного дома» обещают нам комфорт и безопасность, но сами по себе становятся новым фронтом для атак. Умная колонка, которая включает свет по команде, камера, позволяющая следить за домашним питомцем, и Wi-Fi розетка, дистанционно управляющая чайником, — все эти устройства представляют собой мини-компьютеры, подключенные к интернету. И, как любые компьютеры, они имеют уязвимости, превращающие их из помощников в «троянского коня» в вашей крепости.

Определение угроз: уязвимости IoT-устройств как лазейка для злоумышленников

Главная проблема большинства «умных» гаджетов — слабая защищенность «из коробки». Производители часто жертвуют безопасностью ради низкой цены и простоты настройки, что создает ряд критических рисков:

1. Стандартные пароли и уязвимости прошивки: Многие устройства поставляются с логином и паролем типа `admin/admin`, которые пользователи часто не меняют. В интернете существуют целые сканеры, которые автоматически находят такие устройства по всему миру. Кроме того, прошивки редко обновляются, оставляя известные дыры в безопасности незакрытыми.

2. Незашифрованная передача данных: Некоторые дешевые камеры или датчики могут передавать видео и другую информацию по сети в открытом

виде. Это означает, что злоумышленник, перехвативший трафик вашей Wi-Fi сети, может легко получить доступ к этим данным.

3. Доступ к домашней сети: Взлом одного самого простого и уязвимого устройства (например, умной лампочки) может стать плацдармом для атаки на всю вашу сеть. Получив контроль над гаджетом, хакер может перемещаться по сети и атаковать более ценные цели — ваш компьютер, ноутбук или NAS-накопитель с личными фото и документами.

Реальные последствия взлома: от вторжения в частную жизнь до физического ущерба:

1. Шпионаж и вторжение в частную жизнь: Взломанная камера или умная колонка с микрофоном превращается в устройство прослушки и слежки. Злоумышленники могут месяцами наблюдать за вашей жизнью, изучая расписание, подслушивая разговоры и фиксируя, когда дома никого нет.

2. Кража личных данных и шантаж: Получив доступ к вашей сети, хакеры могут похитить пароли от социальных сетей, банковских аккаунтов, личную переписку и интимные фото.

3. Физический ущерб и создание «ботнетов»: Вредоносный код может заставить умные розетки включать и выключать мощные приборы (обогреватели, утюги), вызывая перегрузку сети и пожар. Кроме того, сотни тысяч взломанных «умных» устройств объединяются в «ботнеты» (сети зомби-устройств), которые используются для масштабных кибератак на серверы компаний и правительств.

Защита домашней Wi-Fi сети — ваш цифровой фундамент защиты.

Домашняя Wi-Fi сеть — это не просто источник интернета. Это главная цифровая магистраль, соединяющая все умные устройства в вашем доме. Если эта магистраль не защищена, то все, что по ней передается — ваши пароли, личные переписки, видео с камер — может быть перехвачено.

1. Смена паролей по умолчанию и использование стойкого шифрования

Самые простые действия часто являются самыми эффективными. Производители устанавливают на роутеры и устройства стандартные логины и пароли (admin/admin), которые известны всем, включая злоумышленников.

а) немедленно смените пароль администратора роутера на уникальный и сложный, используя для этого проводное подключение;

б) убедитесь, что в настройках роутера активировано современное шифрование WPA2 или, что лучше, WPA3. Никогда не используйте устаревший и крайне уязвимый стандарт WEP;

в) пароль для подключения к самой Wi-Fi сети также должен быть длинным (не менее 12 символов) и содержать буквы, цифры и специальные знаки.

2. Создание гостевой сети для непроверенных устройств

Гостевая сеть — это не просто удобство для ваших друзей. Это важнейший инструмент изоляции рисков.

а) создайте отдельную гостевую сеть и включайте ее только при необходимости;

б) подключайте к этой сети все устройства гостей, а также свои собственные «подозрительные» или редко используемые гаджеты (например, умную лампочку или старый планшет). Это не позволит им, в случае взлома, получить доступ к основным устройствам вашей сети — компьютерам и NAS-серверам с личными данными.

3. Регулярное обновление прошивки роутера

Прошивка — это операционная система вашего роутера. Как и любое ПО, она содержит уязвимости, которые производитель исправляет с помощью обновлений.

а) включите функцию автоматического обновления прошивки в настройках роутера, если она предусмотрена.

б) проверяйте наличие обновлений на сайте производителя вручную не реже одного раза в квартал. Установка последней версии прошивки закрывает известные дыры в безопасности и является одной из самых действенных мер защиты.

Принцип «слоеной защиты» (Defense in Depth)

Обеспечение безопасности современного жилища по принципу «установил и забыл» не просто наивно, но и опасно. Единственная линия обороны, какой бы надежной она ни казалась, всегда имеет уязвимость. Ключевая стратегия — создание эшелонированной, многоуровневой системы безопасности, где отказ одного элемента не приведет к катастрофе, а будет компенсирован другими.

Классическая ошибка — вера в панацею. «У меня стоит дорогая умная камера, значит, я в безопасности». Однако если злоумышленник взломает вашу Wi-Fi-сеть, он может:

1. Получить доступ к камере и отключить ее прямо в момент проникновения.
2. Изучить через нее ваши привычки и расписание.
3. Использовать ее как точку доступа для атаки на другие устройства.

Пример эффективной комплексной системы

Реализация принципа «слоеной защиты» на практике выглядит как совокупность взаимодополняющих рубежей:

Первый рубеж: Сдерживание и физический барьер.

а) надежная металлическая дверь с противовзломной фурнитурой;

б) два замка разных типов (сувальдный + цилиндровый высокой секретности);

в) противовзломные стеклопакеты на первом этаже.

Второй рубеж: Раннее обнаружение и предупреждение.

а) датчики открытия на окнах и дверях;

б) датчики движения в ключевых зонах, настроенные на режим «охрана».

Эти датчики подключены к автономной сирене и отправляют уведомления на смартфон.

Третий рубеж: Наблюдение, документирование и резервирование.

а) уличная IP-камера с ИК-подсветкой, записывающая видео в облако;

б) камера внутри прихожей с автономным источником питания (Power over Ethernet или встроенным аккумулятором) и, что критично важно, с отдельным сотовым модулем (4G/LTE). Это гарантирует ее работу даже при отключении электроэнергии и интернета.

Человеческий фактор: самый слабый элемент системы

Можно инвестировать в самые передовые технологические решения, но без грамотного и осознанного пользователя вся эта система будет напоминать крепость с открытыми воротами. Человеческий фактор был, есть и остается самым ненадежным звеном в любой системе безопасности. Его ошибки, невнимательность или беспечность сводят на нет эффективность даже самых совершенных устройств.

1. Использование уникальных сложных паролей. Пароль `123456` или `qwerty` — это приглашение для злоумышленника. Для каждого сервиса и устройства должен быть свой пароль, созданный с помощью менеджера паролей. Это исключает эффект домино, когда взлом одной учетной записи приводит к компрометации всех остальных.

2. Обязательное использование двухфакторной аутентификации (2FA). Это критически важный второй барьер. Даже если пароль каким-то образом станет известен, злоумышленник не сможет войти в аккаунт без одноразового кода из приложения-аутентификатора или SMS. Данную функцию необходимо активировать для всех важных сервисов, включая учетную запись умного дома и электронную почту.

3. Повышенная осторожность с фишингом. Нельзя слепо доверять письмам и сообщениям, даже если они выглядят как официальные. Нельзя переходить по подозрительным ссылкам и тем более вводить свои логины и пароли на сайтах, на которые эти ссылки ведут. Прежде чем совершить какое-либо действие, необходимо самостоятельно, а не по ссылке из письма, зайти на официальный сайт службы и проверить информацию.

Заключение

Обеспечение безопасности жилища — это не разовый проект по установке гаджетов, а непрерывный процесс, основанный на осознанном подходе и выработке устойчивых привычек. Технологии — это лишь инструменты, эффективность которых напрямую зависит от того, как ими пользуются. Истинная безопасность достигается тогда, когда правильные действия

становятся автоматическими: закрыть дверь на все замки, не переходить по сомнительным ссылкам, установить обновление. Это и есть культура безопасности — состояние, при котором забота о своей защите становится неотъемлемой и естественной частью повседневной жизни, гарантируя долговременный и надежный результат.

СПИСОК ЛИТЕРАТУРЫ

1. Литвинова, Н. А. Чистота воздуха и вентиляция жилища / Н. А. Литвинова // Экология урбанизированных территорий. – 2008. – № 1. – С. 42-44. – EDN JWBJCV.

2. Пахаев, Х. Х. Анализ технологий построения автоматизированной системы «Умный дом» / Х. Х. Пахаев, Т. Г. Айгумов, Э. М. Абдулмукминова // Инженерный вестник Дона. – 2023. – № 2(98). – С. 1-11. – EDN POGBOS.

3. Смыслов, В. Ю. Анализ угроз информационной безопасности системы "умный дом" / В. Ю. Смыслов // Интернаука. – 2021. – № 44-1(220). – С. 51-53.

4. Кудрявцев, А. В. Методы защиты Wi-Fi сетей от несанкционированного доступа / А. В. Кудрявцев, П. И. Алексеевский // Проблемы естественных, математических и технических наук в контексте современного образования : материалы Международной научно-практической конференции, Липецк, 26–27 октября 2023 года. – Липецк: Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, 2023. – С. 23-29.

5. Bipin Gajbhiye. Defense in Depth Strategies for Zero Trust Security Models / Bipin Gajbhiye, Shalu Jain, Om Goel // International Journal for Research Publication and Seminars. – 2024. – Vol. 15, No. 3. – P. 293-305.

6. Чернышова, В. В. Роль человеческого фактора в системе комплексной безопасности / В. В. Чернышова, С. Н. Рузаев // Совершенствование инженерно-технического обеспечения производственных процессов и технологических систем : Материалы национальной научно-практической конференции с международным участием, посвященной 75-летию основания инженерного факультета ФГБОУ ВО Оренбургский ГАУ, Оренбург, 07 февраля 2025 года. – Оренбург: Оренбургский государственный аграрный университет, 2025. – С. 617-620.