УДК 004.896:658.562.3:628.1

# ОЦЕНКА УРОВНЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ КАЧЕСТВОМ ВОДЫ

**Р. А. Сабиров, С. У. Увайсов**
[1] *Сургутский государственный университет, mr.a.linkoln@mail.ru, uvaysov@yandex.ru*

Выделены особенности функционирования автоматизированных систем управления технологическим процессом (АСУ ТП) контроля качества воды в водооборотных системах (ККВВС) промышленных предприятий (ПП). Исходя из общей системы оценки уязвимостей (CVSS), предложен алгоритм методики оценки угроз информационной безопасности (ИБ) АСУ ТП ККВВС. Получена оценка уровня наиболее распространенных угроз информационной безопасности по критериям исследовательской группы Positive Technologies и показано, что угроза исполнения вредоносного кода является наиболее опасной для нормального функционирования данной системы.

*Ключевые слова:* автоматизированная система управления технологическим процессом, контроль качества воды водооборотных систем, информационная безопасность.

# ESTIMATION OF THREAT LEVEL TO INFORMATION SECURITY OF AUTOMATED WATER QUALITY CONTROL SYSTEMS

**R. A. Sabirov, S. U. Uvaysov**
*Surgut State University, mr.a.linkoln@mail.ru, uvaysov@yandex.ru*

Features of the functioning of automated process control systems for water quality control in water circulation systems of industrial enterprises are singled out. Based on the general system of vulnerability assessment, an algorithm for assessing the threats to information security of the automated process control system for water quality control in water circulation systems is proposed. An estimate of the level of the most common threats to information security upon the criteria of the research group Positive Technologies is derived. It is shown that the threat of malicious code execution is the most dangerous for the normal functioning of this system.

*Keywords:* automated process control system, quality control of water circulation systems, information security.

Вода имеет важное значение и широкое применение в разных технологических процессах на большинстве промышленных предприятиях России и всего мира. Большой объем воды используется для охлаждения производственных агрегатов ПП. При этом в процессе охлаждения агрегатов вода загрязняется и нагревается. Принудительное охлаждение оборотной воды за счет испарения в градирнях и подпитка необработанной водой из природных источников повышают количество солей в системе, изменяя свойства оборотной воды. В ряде случаев экономически оправдано такую воду очищать и остужать, подавая снова для повторного использования. Данный процесс определяет эффективность работы различных теплообменных механизмов и устройств на предприятии. Таким образом, изменение качества воды является фактором, приводящим к снижению производительности процесса. Строительные нормы и правила (СНиП) предусматривают продувание системы, подщелачивание, окисление, осветление добавочной воды и удаление из оборотной системы части взвешенных веществ. Также применяются новые способы защиты: в систему впрыскиваются разнообразные полимерные присадки – реагенты, предотвращающие формирование кальциевидных отложений, ржавчины и биообрастания в элементах водооборота предприятия. Применение АСУ ТП с целью автоматического дозирования и

коррекции подачи реагентов в зависимости от качества оборотной воды способствует поддержания ее постоянных свойств [7].

Сбор данных об используемых АСУ ТП ККВВС затруднено вследствие того, что такие технологии считаются интеллектуальной собственностью создателей и тщательно утаиваются, поддерживая отсутствие конкуренции на рынке.

Функции системы управления разделяются на управляющие и информативные [8] (получение, обработка, передача и преобразование информации), а сами системы можно классифицировать по отличительным особенностям функционирования: по уровню, занимаемому в производственной иерархии; виду протекания ТП; информативной способности; степени функциональной надежности; типу функционирования.

По уровню, занимаемому в производственной иерархии, АСУ ТП ККВВС классифицируется как система с многоуровневой организацией, так как на нижних уровнях приборы измерений собирают данные о количестве примесей в составе воды, а на верхнем уровне – программно-логический контроллер (ПЛК), используя исполнительные устройства, корректирует подачу реагентов.

Вид протекания ТП во времени определяется характером поступления реагентов в систему. Данный процесс является постоянным с безостановочной подачей реагентов в воду.

Информативная способность характеризуется количеством, измеряемых или регулируемых переменных [3]. Система контроля качества воды имеет наименьшую (< 40) информативную способность.

Степень функциональной надежности определяются наличием документов, регламентирующих работу технологического объекта управления (ТОУ).

Тип функционирования АСУ ТП определяет совокупность автоматически исполняемых управляющих и информативных функций [3].

Таким образом, АСУ ТП ККВВС является многоуровневой системой с непрерывным технологическим процессом, имеющую наименьшую информативную способность и среднюю степень функциональной надежности с автоматическим управлением.

К современным АСУ ТП предъявляются высокие требования по защите от угроз ИБ в области обеспечения: конфиденциальности (недопустимость нарушения неправомерного доступа); целостности (защита от несанкционированного изменения); доступности (обеспечению доступности разрешенному объекту).

Цель любой атаки заключается в нарушении либо конфиденциальности, целостности, доступности или нескольких требований ИБ одновременно [4, 7].

Для осуществления угроз ИБ используют уязвимости компонентов АСУ ТП. Так, экспериментально-исследовательская группа Positive Technologies, в период с 2012 по 2015 гг. выявила 743 уязвимости компонентов АСУ ТП. Максимальное количество было найдено в SCADA (Supervisory Control And Data Acquisition – диспетчерское управление и сбор данных), программируемых логических контроллерах (ПЛК), сетевых устройствах промышленного направления и инженерном ПО, а также в компонентах человеко-машинных интерфейсов и терминалах удаленного доступа. Вероятность осуществлении угрозы ИБ и уровень воздействия на ресурсы АСУ ТП характеризуют общий уровень угрозы информационной безопасности (степень критичности для нормального функционирования системы) [4–5].

Наибольшее число угроз (рис. 1) относятся к таким типам, как отказ в обслуживании (29 % от общего числа), выполнение вредоносного кода (21 %), переполнение буфера (20 %) и кража информации (8,8 %). Их реализация приводит к отказу в работе оборудования или к его несанкционированной эксплуатации, что, учитывая требования к нормальному функционированию АСУ ТП, недопустимо [10].

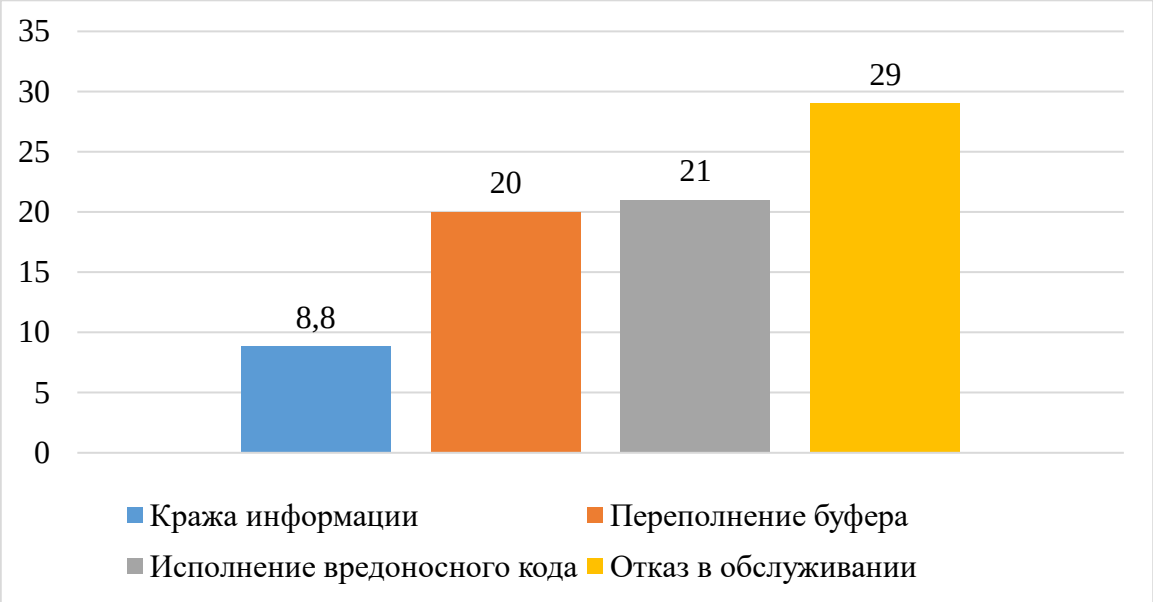


**Рис. 1. Соотношение типов угроз ИБ АСУ ТП**

С целью установления степени влияния угроз ИБ необходимо их ранжировать, т. е. определить, какие угрозы более значимы, а какие менее. Чем выше ранг угрозы, тем она опаснее и тем большую часть ограниченных ресурсов необходимо выделить для ее нейтрализации.

Стандарт системы оценки уязвимостей CVSS предоставляет возможность обработать ключевые характеристики и рассчитать численную оценку, характеризующую ее тяжесть. Численный итог можно перевести в качественные показатели (низкий, средний, высокий и критический). Данный метод помогает организациям верно оценить и расставить приоритеты своих процессов управления [6, 11].

Каждой угрозе ИБ присваивается показатель воздействия и использования, характеризующий степень влияния угрозы ИБ на конфиденциальность, целостность и доступность информации, обрабатываемой в АСУ ТП [9, 11].

Основу CVSS представляет базовая метрическая группа (рис. 2), которая состоит из постоянных во времени характеристик: метрик эксплуатационной способности (Exploitation) и показателей эффективности (Effect) [11].


**Рис. 2. Базовая группа метрик CVSS**

Метрики эксплуатации отражают легкость и технические средства, с помощью которых угрозы могут быть использованы. С другой стороны, показатели воздействия отражают прямое следствие успешного их использования (влияние на конфиденциальность, целостность и доступность) [1, 11].

Метрики эксплуатационной способности состоят из значений. Вектор атаки (VS) отображает ,как угроза эксплуатируется по отношению компонентам АСУ ТП. Вектор атаки может принимать значения:

- 0,395 – в случае, если угроза может быть осуществлена только при наличии локального доступа к ресурсам АСУ ТП [1];

- 0,46 – когда угроза может быть реализована из каналов передачи данных корпоративной сети, через коммуникационный уровень АСУ ТП;

- 1 – в случае, когда угроза может быть реализована извне (например, из Internet).

Сложность (С) – метрика измеряет сложность реализации атаки, которая нужна для осуществления угрозы:

- 0,35 – высокая сложность атаки, когда существуют специальные условия для ее реализации;

- 0,61 – средняя, при недостаточной защищенности АСУ ТП;

- 0,71 – низкая, когда отсутствуют меры защиты АСУ ТП.

Аутентификация (А) – коэффициент показывает сколько раз злоумышленнику нужно пройти проверку подлинности для осуществления угрозы:

- 0,45 – необходима постоянная проверка подлинности для доступа к компонентам АСУ ТП;

- 0,56 – однократная аутентификации;

- 0,704 – проверки подлинности не требуется.

Метрики показателей эффективности: влияние на конфиденциальность (CON), доступность (AVA) и целостность (INT) принимают значения:

- 0 – если угроза не влияет;

- 0,275 – влияние происходит при выполнении определенных условий;

- 0,66 – если угроза влияет.

Функция влияния характеризует актуальность угрозы, 0 – если f(Effect) = 0 и 1,176 – если f(Effect) ≠ 0.

Базовый уровень угрозы (Base Threat Level – BTL) ИБ рассчитывается по формуле:

$$BTL = ((0{,}4 * Exploitation) + (0{,}6 * Effect)) - 1{,}5 * f(Effect) \quad (1)$$ [11].

Произведем расчет BTL для наиболее популярных угроз АСУ ТП ККВВС. Для этого необходимо рассчитать показатели эксплуатации (Exploitation), показатели эффективности (Effect) и функцию влияния, характеризующую актуальность угрозы f (Effect).

Показатель эксплуатации (Exploitation) угроз рассчитывается по формуле:

$$Exploitation = 20 * VS * C * A \quad (2)$$ [11].

Значения метрик (вектора атаки (VS), сложности (С), аутентификации (А), конфиденциальности (CON), доступности (AVA) и целостности (INT)) получены нами методом анализа информации из «Банка данных угроз безопасности информации» с сайта «Федеральной службы по техническому и экспортному контролю» РФ [12].

Для расчета показателя эксплуатации выделенных нами угроз подставим значения метрик из табл.1 в формулу (2):

*Таблица 1*

**Ранжирование угроз ИБ АСУ ТП ККВВС**

| | Вектор атаки (VS) | Сложность (C) | Аутентификация (A) | Метрики показателей эффективности: влияние на конфиденциальность (CON), доступность (AVA) и целостность (INT) |
|---|---|---|---|---|
| Отказ в обслуживании | VS = 1, так как в большинстве случаев угроза реализуется из Internet | C=0,35, так как для осуществления атаки нужны специальные условия | A = 0,704, проверка подлинности не требуется | CON = 0; INT = 0; AVA = 0,66 |
| Исполнение вредоносного кода | VS = 0,395, так как для реализации необходим локальный доступ к ресурсам и компонентам АСУ ТП | C = 0,71, отсутствует специальные меры защиты | A = 0,56, необходима однократная проверка подлинности для реализации угрозы | CON = 0,66; INT = 0,66; AVA = 0,66 |
| Переполнение буфера | VS = 0,46, так как угроза реализуется из каналов передачи данных корпоративной сети | C = 0,61. | A = 0,704 | CON = 0; INT = 0; AVA = ,66 |
| Кража информации | VS = 0,395 | C = 0,35. | A = 0,45, так как необходима постоянная проверка подлинности для доступа к компонентам АСУ ТП | CON = 0,66; INT = 0; AVA = 0 |

В результате значения показателя эксплуатации для данных угроз будут равны следующим значениям:

$Exploitation(\text{Отказ в обслуживании}) = 5;$

$Exploitation(\text{Исполнение вредоносного кода }) = 3{,}2;$

$Exploitation(\text{Переполнение буфера}) = 3{,}8;$

$Exploitation(\text{Кража информации}) = 1{,}3.$

Подставив полученные значения в диаграмму (рис. 3), мы получили схожую с рис. 1 картину. Угроза отказа в обслуживании получила наибольшую оценку, а угроза кражи информацию – наименьшую. Следовательно, можно сделать вывод, что количество реализованных угроз имеет зависимость от показателя эксплуатации, чем он выше, тем

больше количество реализованных угроз, и наоборот, чем ниже показатель эксплуатации, тем ниже общее количество угроз.

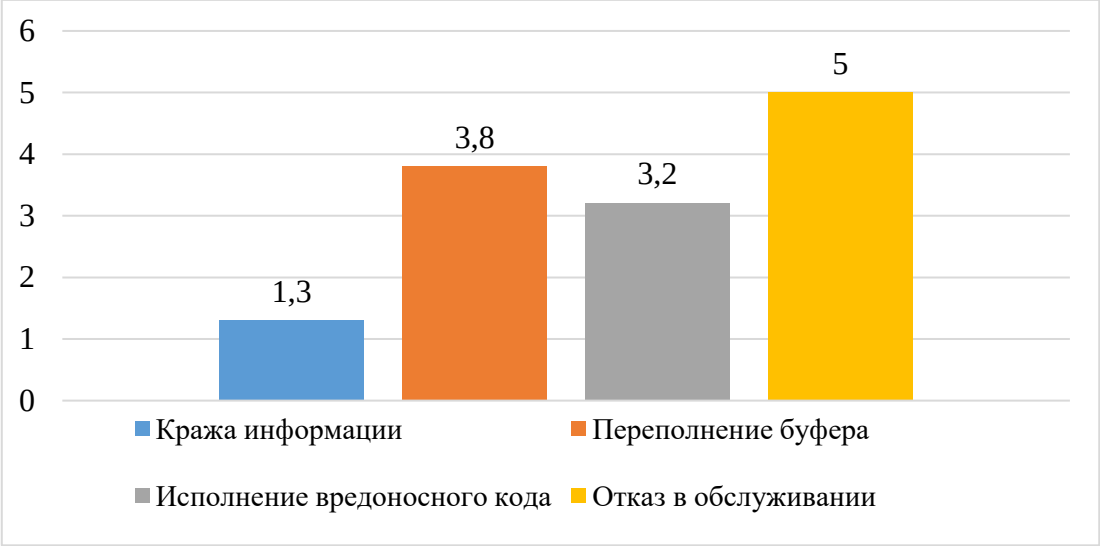


**Рис. 3. Соотношение показателя эксплуатации угроз ИБ АСУ ТП ККВВС**

Расчет показатель эффективности (Effect) рассчитывается по формуле (3). Значения метрик конфиденциальности (CON), доступности (AVA), целостности (INT) для каждой угрозы подставляются из табл. 1:

$$Effect = 10{,}41 * (1 - (1 - CON) * (1 - AVA) * (1 - INT)) \quad (3), [11]$$

$Effect(\text{Отказ в обслуживании}) = 6{,}9;$

$Effect(\text{Исполнение вредоносного кода}) = 10;$

$Effect(\text{Переполнение буфер}) = 6{,}9;$

$Effect(\text{Кража информации}) = 6{,}9.$

Расчет показателей эффективности показал, что угроза «Исполнение вредоносного кода» имеет самую высокую оценку, данный факт объясняется вредоносным воздействием данной угрозы одновременно на 3 направления нарушений требований ИБ (конфиденциальность, целостность и доступность).

Функция влияния f ($Effect$) характеризует актуальность угрозы, f ($Effect$) = 0, если $Effect$ =0 и f ($Effect$) = 1,176, если $Effect \neq 0$.

Подставив полученные значения показателей эксплуатации, эффективности в формулу (1), получим базовую оценку уровня данных угроз:

$BTL(\text{Отказ в обслуживании}) = 4{,}3;$

$BTL(\text{Исполнение вредоносного кода}) = 5{,}5;$

$BTL(\text{Переполнение буфера}) = 4;$

$BTL(\text{Кража информации}) = 2{,}9.$

Угроза «Исполнение вредоносного кода» имеет наиболее высокую оценку, данный факт объясняется наносимым уроном (высоким показателем эффективности (Effect)) при ее осуществлении.

Проведя анализ наиболее популярных угроз АСУ ТП по описанному выше методу, учитывая отличительные признаки работы системы контроля воды водооборотных систем от других АСУ ТП, можно установить, что наиболее опасной является угроза «Исполнение вредоносного кода», получившая высокую оценку (5,5). В случае, если опасность некоторой атаки будет недооценена, то разработчики систем информационной безопасности АСУ ТП не предпримут эффективных мер защиты от этой атаки, что может привести к большому ущербу для владельца программного продукта, его пользователей или его правообладателя. В случае, если опасность атаки будет переоценена, то это может привести к ложной необходимости разработки усиленных мер, что означает трату дополнительных временных и человеческих ресурсов.

**Литература**

1. Кирсанов С. В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли // Докл. ТУСУРа. 2013. № 2. С. 112–115.

2. Финогеев А. Г., Нефедова И. С., Тхай К. В. Проблемы безопасности беспроводной сенсорной сети в SCADA-системах АСУ ТП // Изв. ВолгГТУ. 2014. № 15 (165). С. 66.

3. Втюрин В. А. Основы АСУ ТП. СПб. : СПбГЛТУ им. Кирова, 2006. 153 с.

4. Сабиров Р. А., Увайсов С. У. Information security status analysis of automated process control systems in fuel and energy // Information innovative technologies : International Scientific-Practical Conference, 2017. Прага, 2017. С. 476–478.

5. Сабиров Р. А., Увайсов С. У. Применение средств обеспечения информационной безопасности в промышленных системах управления // Север России: стратегии и перспективы развития : материалы III Всерос. науч.-практич. конф. Сургут, 2017. С. 140–143.

6. Основные принципы создания замкнутых водооборотных систем // Vseokraskah.net. URL: http://vseokraskah.net/ (дата обращения: 11.11.2017).

7. Создание замкнутых водооборотных систем. URL: https://knigi.link/ekologiya/ (дата обращения: 12.11.2017).

8. Безопасность информационных систем и защита информации. URL: http://www.studmed.ru/docs/ (дата обращения: 15.11.2017).

9. Математика криптографии и теория шифрования. URL: https://www.intuit.ru/ (дата обращения: 19.11.2017).

10. Мощнее Stuxnet и Flame: «Лаборатория Касперского» обнаружила самого сильного на данный момент игрока в мире кибершпионажа // Kaspersky.ru : сайт. URL: https://www.kaspersky.ru/ (дата обращения: 20.11.2017).

11. Полное руководство по общей балльной системе уязвимости. URL: https://www.first.org/cvss/v2/guide (дата обращения: 27.12.2017).

12. Банк данных угроз безопасности информации федеральной службы по техническому и экспортному контролю. URL: https://bdu.fstec.ru/ (дата обращения: 04.01.2018).